Reports and Working Papers of the Law Reform Commission of Canada

Reports to Parliament

1. *Evidence* (December 19, 1975)
2. *Guidelines — Dispositions and Sentences in the Criminal Process** (February 6, 1976)
3. *Our Criminal Law* (March 25, 1976)
4. *Expropriation** (April 8, 1976)
5. *Mental Disorder in the Criminal Process** (April 13, 1976)
6. *Family Law** (May 4, 1976)
7. *Sunday Observance** (May 19, 1976)
8. *The Exigibility to Attachment of Remuneration Payable by the Crown in Right of Canada** (December 19, 1977)
9. *Criminal Procedure — Part I: Miscellaneous Amendments** (February 23, 1978)
10. *Sexual Offences** (November 29, 1978)
11. *The Cheque: Some Modernization** (March 8, 1979)
12. *Theft and Fraud** (March 16, 1979)
13. *Advisory and Investigatory Commissions** (April 8, 1980)
14. *Judicial Review and the Federal Court** (April 25, 1980)
15. *Criteria for the Determination of Death* (April 8, 1981)
16. *The Jury* (July 28, 1982)
17. *Contempt of Court** (August 18, 1982)
18. *Obtaining Reasons before Applying for Judicial Scrutiny — Immigration Appeal Board* (December 16, 1982)
19. *Writs of Assistance and Telewarrants* (July 22, 1983)
20. *Euthanasia, Aiding Suicide and Cessation of Treatment* (October 11, 1983)
21. *Investigative Tests: Alcohol, Drugs and Driving Offences* (November 10, 1983)
22. *Disclosure by the Prosecution* (June 15, 1984)
23. *Questioning Suspects* (November 19, 1984)
24. *Search and Seizure* (March 22, 1985)
25. *Obtaining Forensic Evidence* (June 12, 1985)
26. *Independent Administrative Agencies: A Framework for Decision Making* (October 23, 1985)

Working Papers

1. *The Family Court** (1974)
2. *The Meaning of Guilt: Strict Liability** (1974)
3. *The Principles of Sentencing and Dispositions** (1974)
4. *Discovery** (1974)
5. *Restitution and Compensation** (1974)
6. *Fines** (1974)
7. *Diversion** (1975)
8. *Family Property** (1975)
9. *Expropriation** (1975)
10. *Limits of Criminal Law: Obscenity: A Test Case* (1975)
11. *Imprisonment and Release** (1975)
12. *Maintenance on Divorce** (1975)
13. *Divorce** (1975)
14. *The Criminal Process and Mental Disorder** (1975)
15. *Criminal Procedure: Control of the Process** (1975)
16. *Criminal Responsibility for Group Action** (1976)
17. *Commissions of Inquiry: A New Act** (1977)
18. *Federal Court: Judicial Review** (1977)
19. *Theft and Fraud: Offences* (1977)
20. *Contempt of Court: Offences against the Administration of Justice* (1977)
21. *Payment by Credit Transfer* (1978)
22. *Sexual Offences** (1978)
23. *Criteria for the Determination of Death** (1979)
24. *Sterilization: Implications for Mentally Retarded and Mentally Ill Persons* (1979)
25. *Independent Administrative Agencies* (1980)
26. *Medical Treatment and Criminal Law* (1980)
27. *The Jury in Criminal Trials** (1980)
28. *Euthanasia, Aiding Suicide and Cessation of Treatment* (1982)
29. *The General Part: Liability and Defences* (1982)
30. *Police Powers: Search and Seizure in Criminal Law Enforcement** (1983)
31. *Damage to Property: Vandalism* (1984)
32. *Questioning Suspects* (1984)
33. *Homicide* (1984)
34. *Investigative Tests* (1984)
35. *Defamatory Libel* (1984)
36. *Damage to Property: Arson* (1984)
37. *Extraterritorial Jurisdiction* (1984)
38. *Assault* (1985)
39. *Post-seizure Procedures* (1985)
40. *The Legal Status of the Federal Administration* (1985)
41. *Arrest* (1985)
42. *Bigamy* (1985)
43. *Behaviour Alteration and the Criminal Law* (1985)
44. *Crimes against the Environment* (1985)
45. *Secondary Liability* (1985)
46. *Omissions, Negligence and Endangering* (1985)

The Commission has also published over seventy Study Papers on various aspects of law. If you wish a copy of our catalogue of publications, please write to: Law Reform Commission of Canada, 130 Albert Street, Ottawa, Ontario K1A 0L6, or Suite 310, Place du Canada, Montréal, Québec, H3B 2N2.

---

* Out of print. Available in many libraries.

ELECTRONIC SURVEILLANCE

Available by mail free of charge from:

Law Reform Commission of Canada
130 Albert St., 7th Floor
Ottawa, Canada
K1A 0L6

or

Suite 310
Place du Canada
Montréal, Québec
H3B 2N2

© Law Reform Commission of Canada 1986
Catalogue No. J32-1/47-1986
ISBN 0-662-53886-2

Law Reform Commission
of Canada

Working Paper 47

ELECTRONIC SURVEILLANCE

1986

Commission

Mr. Justice Allen M. Linden, President
Mr. Gilles Létourneau, Vice-President*
Ms. Louise Lemelin, Q.C., Commissioner
Mr. Joseph Maingot, Q.C., Commissioner
Mr. John Frecker, Commissioner*

Acting Secretary

Harold J. Levy, LL.B., LL.M.

Co-ordinator, Criminal Procedure

Stanley A. Cohen, B.A., LL.B.

Consultants

Marc Rosenberg, B.A., LL.B.
David Watt, Q.C., B.A., LL.B.

* Was not a member of the Commission when this document was approved.

Notice

This Working Paper presents the views of the Commission at this time. The Commission's final views will be presented later in its Report to the Minister of Justice and Parliament, when the Commission has taken into account comments received in the meantime from the public.

The Commission would be grateful, therefore, if all comments could be sent in writing to:

Secretary
Law Reform Commission of Canada
130 Albert Street
Ottawa, Canada
K1A 0L6

Table of Contents

CHAPTER ONE: Historical Perspective 1

I. The Common Law Position 1

II. The Ouimet Committee 2

III. Federal Protection of Privacy Legislation 3

A. Bill C-176 3

B. Bill C-51 4

CHAPTER TWO: A Case for Reform 7

I. Introduction 7

II. The Constitutional Framework 8

III. The Balance between Respect for Privacy and Effective Law Enforcement 10

IV. The Role of the Judiciary 11

CHAPTER THREE: Our Recommendations and Commentary 13

I. Application of Part IV.1 of the *Criminal Code* 13

A. The Offence 13

B. Private Communications 16

C. Optical Devices 21

D. Foreign Interceptions 23

E. Participant Monitoring: Consent Interceptions 26

II. The Authorization 30
A. The Application Procedure 30
B. Basis for Granting the Authorization 31
C. Interprovincial Offences 32
D. Minimization 34
E. Basket Clauses 39
F. Surreptitious Entry 43
G. Renewals 49

III. Reviewability and Secrecy 52
A. Introduction 52
B. Review of the Authorization 53
C. Secrecy 59
D. Conclusion 62
(1) Issue One: Where Is the Question Resolved? 63
(2) Issue Two: How Is the Question Resolved? 64

IV. Emergency Authorization: Section 178.15 65

V. Remedies 67
A. Admissibility of Evidence of Other Offences 67
B. For Breach of the Statutory Scheme 70
(1) Introduction 70
(2) The Problem of Exclusion Generally 71
C. Notice under Subsection 178.16(4) 73
D. Substantive Defect in the Application 74
(1) Tort Remedy 80
(2) Criminal Liability 80
(3) Extrajudicial Controls 81
(4) Exclusionary Rule 81
E. Derivative Evidence 84
F. The Length of Proceedings 87

VI. Miscellaneous Recommendations 89
A. Annual Reports: Section 178.22 89

B. Notice under Section 178.23 90
C. The Disclosure of Intercepted Private Communications 93
D. Assistance in the Execution of Orders 95

CHAPTER FOUR: Summary of Recommendations 97

CHAPTER ONE

Historical Perspective

I. The Common Law Position

The common law has not recognized the privacy of the individual as a discreet legal interest to be afforded specific legal protection. Neither before the advent of modern electronic technology, not thereafter, with the consequent proliferation of surveillance devices, has such a distinct interest in the protection of privacy emerged. Although a number of civil remedies[1] and criminal prosecutions[2] may incidentally afford some protection of the privacy interest, these have as their primary focus other legally protected interests[3] and were considered inadequate in several respects. First, they fail to afford relief to the essence of an invasion of privacy, namely the invasion of one's thoughts, emotions and sensitivities. Instead, they insisted upon a "precondition of proving actual harm beyond insult or hurt" which rendered "most of the old common law torts irrelevant to protecting the intimate interests that may be at stake in defence of individual privacy."[4] Secondly, the criminal law remedies, prosecution for breaches of the *Criminal Code*, were equally inadequate to the task. Their focus, as well, was not upon privacy interests, and any recognition thereby given or remedy thereby afforded, but was primarily directed towards other criminally protected interests.[5] Thirdly, both civil and criminal remedies were anachronistic in view of modern technological advances which permit trespassory invasion without the commission of a trespass and, *a fortiori*, a criminal offence, in conventional terms.[6]

---

1. For example, trespass, nuisance and negligence actions in relation to the person, chattels or land of the plaintiff.
2. See, for example, *R.* v. *Chapman and Grange*, [1973] 2 O.R. 290, 11 C.C.C. (2d) 84 (C.A.). D's conduct may also engage the prohibitions of paragraph 381(1)(c) or (*f*) of the *Code*.
3. For example, the right to enjoyment of one's land enforced by actions in trespass or nuisance.
4. Law Reform Commission of Australia, *Privacy and Intrusions*, [Discussion Paper No. 13] (June, 1980), pp. 24-5.
5. For example, the integrity of contractual and trading relations in Part VIII of the *Criminal Code*, R.S.C. 1970, c. C-34, or the rights of property in Parts VII and IX.
6. Canadian Committee on Corrections, *Report of the Canadian Committee on Corrections, Toward Unity: Criminal Justice and Corrections*, Roger Ouimet, Chairman (Ottawa: Information Canada, 1969), p. 81 (hereinafter cited as the Ouimet Report).

Finally, the principal concern of the common law of evidence is with relevance rather than the manner in which the evidence is obtained. That which is relevant is legally admissible irrespective of the manner in which it has been obtained,[7] provided, of course, it does not contravene any of the exclusionary canons of the law of evidence. The discretion to exclude evidence, otherwise admissible, remains quite limited.[8] Evidence obtained in consequence of invasions of privacy, as for example by the surreptitious recording of telephonic communications, is admissible at common law. This is so notwithstanding the unlawfulness of the conduct used to obtain the evidence, provided it is relevant and properly authenticated.[9]

II. The Ouimet Committee

In its 1969 report, the Ouimet Committee[10] considered that the "interest" which required protection by federal legislation was the privacy of conversations taking place under such circumstances as to justify a reasonable belief on the part of *both* parties that such conversations were not subject to acquisition by others through the use of electronic, mechanical or other devices.[11] As an exception, law enforcement interceptions of private conversations should be permitted, subject to specific conditions and constraints.[12] The Committee would exempt from the scheme of legislative control participant monitoring (consent recording), listening in on extensions and acquiring the contents of conversations taking place in circumstances denuded of any justifiable expectation of privacy.[13] The Committee favoured a system of judicial control of wiretapping and electronic eavesdropping and outlined a proposed scheme in this regard.[14]

The issue of the admissibility of conversations obtained through wiretapping and electronic surveillance was considered. The Committee, which had recommended against a rigid rule excluding all other illegally obtained evidence in favour of a discretion to exclude such evidence, suggested that a separate rule providing for the inadmissibility of such evidence should govern the admissibility of illegally intercepted conversations in view of the unlikelihood of error or inadvertence accounting for such interceptions.[15]

Shortly stated, the Ouimet Committee concluded that as wiretapping and electronic eavesdropping for criminal purposes ought to be suppressed by criminal legislation, so too should its evidentiary fruits. At the same time, the Committee recognized that

7. *Kuruma* v. *The Queen*, [1955] A.C. 197 (P.C.).
8. *R.* v. *Wray*, [1971] S.C.R. 272, [1970] 4 C.C.C. 1.
9. The principal focus of the earlier cases was upon the adequacy of the proof of such issues.
10. Ouimet Report, *supra*, note 6.
11. *Id.*, pp. 82-3.
12. *Id.*, p. 83.
13. *Id.*, p. 85.
14. *Id.*, p. 86.
15. *Id.*, pp. 87-8.

effective law enforcement required electronic surveillance as an investigative aid or tool. While prepared to create an exception for such purposes, the Committee made it plain that such surveillance should require prior judicial authority and be subject to strict control.[16]

III. Federal Protection of Privacy Legislation

The need for federal legislation to control wiretapping and electronic eavesdropping, as identified in the Ouimet Report, assumed legislative form in the proclamation of the *Protection of Privacy Act*[17] on June 30, 1974.

A. Bill C-176

On April 13, 1973, the Minister of Justice introduced Bill C-176 in the House of Commons. The pervasive quality of warranted electronic surveillance was maintained in Bill C-176 by its adopting the same definition of "offence" as was in Bill C-252, namely:

> "offence" means an offence created by an Act of the Parliament of Canada for which an offender may be prosecuted by indictment and includes any such offence that is alleged or suspected or that there are reasonable grounds to believe may be committed; ....

Also, the proposals maintained a distinction between the principles applicable to the admissibility of primary evidence and those which determined whether derivative evidence would be received. In the former instance, inadmissibility was the rule, admissibility the exception. Concerning derivative evidence, the opposite appeared to be so.[18]

Bill C-176 was openly debated at length. Many proposals for amendment were moved, although most of these were defeated.[19] There are but three amendments which merit further comment.

Upon first reading, Bill C-176 had defined "offence" in section 178.1 of the *Criminal Code* in such a way as to include breaches of any federal statute for which an offender may be prosecuted by indictment[20] as well as any such offence that was

16. It was proposed, for example, that the tapes of the conversations recorded pursuant to the order be returned to the authorizing judge.

17. S.C. 1973-74, c. 50.

18. The derivative evidence was said to be inadmissible not solely because the primary evidence from where it was derived was itself excluded.

19. One proposal, in effect, would have limited warranted electronic surveillance to *Official Secrets Act* (R.S.C. 1970, c. O-3) or national security matters.

20. The effect of paragraph 27(1)(*a*) of the *Interpretation Act*, R.S.C. 1970, c. I-23, is also to include dual procedure or Crown option offences in the definition.

alleged or suspected or that there were reasonable grounds to believe may be committed. The definition of "offence" was amended to include a catalogue of offences viewed as sufficiently serious in themselves, particularly appropriate for the use of electronic surveillance, or reflective of the activities of organized crime. The definition not only listed substantive offences but also conspiracies, attempts, or being an accessory after the fact to such listed offences. The final element of the definition was a somewhat circular inclusion: "organized crime."[21] It was felt that the narrower focus of the amended definition, passed by the House, would have a limitary effect upon the intrusive nature of the investigative technique.

Secondly, the House substituted a new section 178.15 for the emergency authorization provision which had earlier been proposed. The initial proposal had not involved, save in an *ex post facto* manner, any judicial officer, but rather had provided for the issuance of emergency permits by the Attorney General of a province, the Solicitor General of Canada or their respective agents specially designated in writing for such purpose. The amendments passed in the House, required approval by a judge and resulted in the present scheme of emergency authorization.

The final amendment made in the House, relates to the admissibility of primary and derivative evidence. The House added, by subsection 178.16(3), a provision whereby both primary and derivative evidence might be admitted, notwithstanding certain formal or procedural defects in the authorization process. It was apparently felt that the additional sanction of the exclusion of credible and relevant evidence was not warranted in view of the criminal prohibition in subsection 178.11(1) of the *Code*.[22]

The *Protection of Privacy Act* remains, at least in several of its most significant aspects, in substantially the same form today as it did at the time of its proclamation on June 30, 1974. The most extensive amendments[23] made to the original legislation obtained final Commons approval on July 18, 1977, and became effective on October 15, 1977. Some of those amendments touch upon matters in respect of which we recommend changes in the present law, so it becomes necessary here to record some brief observations.

B. Bill C-51

Bill C-51 replaced the definition of "offence" by an amendment which listed a variety of substantive offences,[24] included counselling, procuring, inciting, conspirary, attempt and being an accessory after the fact to such offences, as well as a definition of "organized crime."

---

21. "And that such pattern is part of the activities of organized crime."

22. See, for example, *House of Commons Debates*, First Session, Twenty-ninth Parliament, 22-23 Elizabeth II, Vol. VIII, November 27, 1973, p. 8203 ff.

23. Bill C-51 received first reading on April 20, 1977.

24. The new offences, not all punishable by imprisonment for five years or more, included the crimes in ss. 88, 111, 112, 127, 132, 133(1), 144, 159(1)(*a*), 185(1), 195(1)(*a*) and 340 of the *Criminal Code*, R.S.C. 1970, c. C-34.

The expansion of the definition of "offence" in section 178.1 was also accompanied by an increase in the length of the authorization and renewal periods from the original thirty to sixty days.[25] The proposed increase was founded essentially upon statistical data which demonstrated the average length of warranted interceptions to be in the vicinity of sixty days.[26]

Bill C-51, also added paragraphs (*e*) and (*e*.1)[27] to subsection 178.12(1) making mandatory disclosure, in the supportive affidavit, of the occupations of all proposed named objects of interception, if known. Further, details of any previously unsuccessful or withdrawn applications in relation to a named object and offence have to be disclosed. The purpose of requiring occupational disclosure was linked to the proposals limiting the right to intercept solicitors' communications.[28] The object of the proposals requiring disclosure of unsuccessful and withdrawn applications was at least to control judge shopping.[29]

Finally, Bill C-51 proposed and enacted significant changes to the evidentiary rules applicable in the event that derivative evidence is tendered for admission. The principal change, premised on expediency in the conduct of criminal trials, removed derivative evidence from the reach of the exclusionary rule and made it *prima facie* admissible, subject to the right of the presiding judicial officer to exclude it if its admission would bring the administration of justice into disrepute.[30] The principles upon which primary evidence fell to be admitted were altered only slightly to make it plain that the mere fact that the evidence was tendered in proceedings for an offence other than one authorized in the judicial warrant did not render the evidence inadmissible.[31]

---

25. No distinction was drawn between authorizations and renewals in this respect.

26. It is arguable that although the amendment had the potential effect of increasing the period over which privacy was invaded, it did so by virtue of an authorization granted upon a more stringent basis than that for renewals.

27. Paragraph 178.12(1)(*e*.1) was not included in the original Bill.

28. Bill C-51, subsections 178.13(1.1) and (1.2).

29. The "solicitor" amendments are at once too wide and too narrow: the former, *inter alia*, because they are not limited to solicitor-client communications, and the latter because they only relate to the "solicitor" half of the problem. The "judge-shopping" amendment only requires disclosure in the event of an earlier failure or withdrawal: the real problem is to prevent the "favourable judge" from being selected in the first instance.

30. Bill C-51, subsection 178.16(1).

31. Subsection 178.16(4) in Bill C-51 as passed: now subsection 178.16(3.1) of the *Code*. It is doubtful if this provision changed the law, at least in those jurisdictions which followed *R.* v. ***Welsh and Iannuzzi (No. 6)*** (1977), 15 O.R. (2d) 1, 32 C.C.C. (2d) 363 (Ont. C.A.).

CHAPTER TWO

A Case for Reform

I. Introduction

The legislation which enacted Part IV.1 of the *Criminal Code*[32] was presented by the Minister of Justice as legislation to protect the privacy of individuals. It was to be an offence to intercept private communications, disclose private communications and to possess equipment for the purpose of intercepting private communications. However, a case had been made out for the use of electronic surveillance by the police to combat crime; therefore, ancillary to the offence-creating sections was a scheme for judicial authorization of interceptions.

Since the enactment of the legislation, there has been only a handful of prosecutions for the offences in Part IV.1, of which most, if not all, concerned possession of interception devices. Moreover, in some instances the devices involved have been merely police scanners rather than sophisticated interception equipment. On the other hand, there have since been many thousands of authorized wiretaps. The Supreme Court of Canada, in *Goldman* v. *The Queen*,[33] observed that it may be more realistic to say that the purpose or effect of Part IV.1 has been to regulate the method of breach of any such right.

The case for reform in the area of electronic surveillance can be made on two levels. Broadly speaking, there has been an increasing concern as to whether or not the legislation does, in fact, protect persons' legitimate expectations of privacy. The recent enactment of the *Canadian Charter of Rights and Freedoms*[34] brings this concern into sharper focus. Electronic surveillance is a particularly intrusive form of investigation and should be used only in special circumstances where other less intrusive methods would be ineffective. It is a technique which should be employed with restraint. In our consultations throughout Canada, there was no dissent from the proposal that use of electronic surveillance must be accompanied by restraint; nor was there a consensus as to whether the present statutory scheme was being administered with restraint.

---

32. This and all references to the *Criminal Code* pertain to R.S.C. 1970, c. C-34, as amended.

33. *Goldman* v. *The Queen*, [1980] 1 S.C.R. 976, p. 994; 51 C.C.C. (2d) 1, p. 15, *per* McIntyre J.

34. *Canadian Charter of Rights and Freedoms*, *Constitution Act, 1982*, as enacted by the *Canada Act 1982* (U.K.), c. 11.

The narrower concern is with the mechanics of the legislation. Part IV.1 of the *Criminal Code* is a technical piece of legislation giving rise to initial problems of interpretation. Thus, while the principles of restraint and respect for privacy are important, it is also important that the powers provided to the police be clearly defined "to facilitate the conduct of criminal investigations ... without unreasonably or arbitrarily interfering with individual rights and freedoms."[35]

As this Working Paper is part of the Police Powers Project, it is appropriate that we also be realistic about the legislation: accordingly our primary concern is to define the limits of lawful breach of the "right" to privacy. Thus, the focus of this Paper is the use by police of this method of investigation, not the offence-creating sections. Such reference to the offences is only incidental to the regime of regulation, and is not properly part of our mandate in this Working Paper.

We do not consider that a total overhaul of the present legislative scheme is necessary. The legislation is very recent and, unlike other areas of police powers, tends to reflect twentieth century values and principles rather than those of the seventeenth, eighteenth or nineteenth century. Thus, implicit in the legislation are the principles of restraint, respect for privacy, definition of the powers of the police and judicial review. Where the legislation has failed to accord with these principles in a manner which can be justified by the balancing of interests, we nevertheless believe such problems can be resolved within the framework of the present legislation.

II. The Constitutional Framework

That electronic surveillance is subject to scrutiny under section 8 of the *Canadian Charter of Rights and Freedoms*,[36] which provides that "[e]veryone has the right to be secure against unreasonable search or seizure," is now placed beyond dispute by reason of the Supreme Court of Canada's decision in *Hunter* v. *Southam Inc.*[37] In this judgment, Chief Justice Dickson adopted an approach to section 8 of the Charter premised on the decision of the United States Supreme Court in *Katz* v. *United States*[38] that section 8, like the Fourth Amendment to the United States Constitution, protects the individual's reasonable expectation of privacy and requires a balance between an individual's privacy and the government's interest in law enforcement.[39]

The adoption of the *Katz* reasonable expectation of privacy test is particularly significant for this study, since *Katz* was in fact a wiretap case where the United States Supreme Court held that electronic eavesdropping was within the Fourth Amendment

35. Government of Canada, *The Criminal Law in Canadian Society* (Ottawa: Government of Canada, 1982), p. 61.

36. *Supra*, note 34.

37. *Hunter* v. *Southam Inc.* (1984), 14 C.C.C. (3d) 97 (S.C.C.).

38. *Katz* v. *United States*, 389 U.S. 347 (1967).

39. *Supra*, note 37, p. 128.

protection against unreasonable search and seizure. In the defining of limits to constitutional protection dependent on an assessment of the impact of the government intrusion, one useful guide "is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society."[40] Electronic surveillance obviously comes within that kind of test.

The other significant aspect of the *Hunter* v. *Southam Inc.* case is the court's policy decision to opt for the requirement of prior authorization such as a warrant, except where a warrantless intrusion can be justified. Further, the court requires that the assessment of the competing interests be on a sliding scale depending on the type of intrusion and the state interest involved. The court adopts the "probable cause" standard under section 8 of the Charter for ordinary law enforcement.

As Chief Justice Dickson stated: "The State's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion."[41] In our view, this may have implications in the electronic surveillance context, particularly as regards the validity of "basket clauses," the definition of "private communication," warrantless installation of optical devices, access to material used on the application and minimization, to name just a few. In the one pre-*Hunter* case where it was held that Charter section 8 did apply to electronic eavesdropping, Ewaschuk J. accepted that "the Canadian legislative scheme would violate U.S. constitutional requirements" but that this was reasonable noting that "Canadian legal tradition has, however, traditionally struck the balance more in favour of society than has American tradition."[42] While Ewaschuk J.'s reading of the pre-Charter mood may be correct, we doubt whether the balance under the Charter is now so weighted in favour of "society" (that is, intrusion). It is to be noted that Chief Justice Dickson identified the privacy interest protected by section 8 not with the individual, but with society, to be balanced against the government interest in law enforcement. As he said earlier in the judgment, the constitutionality of a search or seizure must focus on its reasonable or unreasonable impact on the subject of the search or the seizure "and not simply on its rationality in furthering some valid government objective."[43]

The enactment of the *Canadian Charter of Rights and Freedoms* requires that the legislation be scrutinized with care and that we be alive to potential arguments that certain provisions could offend section 8.

---

40. A.G. Amsterdam, "Perspectives on the Fourth Amendment" (1974), 58 *Minn. L. Rev.* 349, p. 403.
41. *Supra*, note 37, pp. 114-5.
42. *R.* v. *Rowbotham* (1984), 42 C.R. (3d) 164 (Ont. H.C.J.), p. 170.
43. *Supra*, note 37, p. 106.

III. The Balance between Respect for Privacy and Effective Law Enforcement

As we have seen, Part IV.1 of the *Criminal Code*, when originally enacted, was directed at suppression of unlawful wiretapping and control of official electronic eavesdropping. It was absolutely clear that resort to wiretapping and other forms of electronic eavesdropping investigation was to be exceptional. Since the enactment of Part IV.1, and particularly since the 1977 amendments, there has been concern that electronic eavesdropping has been used with far greater frequency than was originally intended and with far fewer restrictions than were envisaged. This concern takes two forms: review of the statistical data in the annual reports, usually in comparison to the American statistics; and secondly, anecdotal reports — use of wiretaps in circumstances which are perceived as trivial or where other less intrusive investigative measures would have succeeded. Unfortunately, the secrecy provisions of Part IV.1, section 178.14, prevent us from directly applying our own judgment to the problem. In any event, since there is no institutionalized objective review of the investigations, other than the limited statistics in the annual reports, it would be difficult to measure the reality of these concerns. The anecdotal "evidence" is suspect since it is so subjective. What defence counsel perceives as a trivial use of the wiretap power may simply be a failure of proof of the important aspect of the investigation.

There are obviously dangers which attend the use of statistics, but certain observations should be recorded. Notwithstanding that the Canadian legislation is similar to, and is in fact based upon, the American legislation, the relative number of authorizations in Canada is nearly twenty to one.[44] Even if we accept that the American legislation is more restrictive, this seems to be an astonishing difference. Furthermore, while section 178.13 contemplates that the authorizing judge will impose terms and conditions, such are virtually never included in the authorization. On the other hand, without our intending to be unduly critical of the judiciary, "basket clauses" have become increasingly wider and almost universal in authorizations.

---

44. This comparison is based on the 1981 statistics compiled pursuant to section 178.22 of the *Criminal Code* for Canada and by the Administrative Office of the United States Courts for the United States. The figure for Canada is 1,059 and for the United States 589. It should be pointed out that this pattern has remained consistent. Thus, see for example, Louise Savage, "An Analysis of the Federal and Provincial Annual Reports relating to the Use of Court Authorized Electronic Surveillance by Law Enforcement Officials in Canada" (unpublished study prepared for the Law Reform Commission of Canada, 1979), where the figures are set out as follows:

	U.S.	*Canada*
1975	701	1,123
1976	686	1,218
1977	626	1,304

This is despite the fact that, as a result of the 1977 amendments, the maximum length of authorizations was increased from thirty days to sixty days, whereas in the United States the maximum period has remained at thirty days. It should be noted that there were "relatively" fewer renewal applications in Canada (205) while extensions were granted 208 times in the United States.

In our view, the substantial reason for difference in the relative use of the technique between Canada and the United States is that in Canada it is much more cost-effective. It has become clear from consultations with law enforcement authorities in the United States and Canada that wiretapping is an extremely costly and time-consuming business in the United States, as the result of monitoring devices and additional paperwork. There may, of course, be other reasons such as greater disclosure requirements causing the authorities to forego projects which would expose the identities of informants, centralized control over the applications, at least in the federal system, which tends to reduce the number of applications which go forward, and the fact that some states actually prohibit wiretapping.

The obvious implication of the foregoing discussion is that there is a great need for openness in the process. Accordingly, we have approached many of the provisions from the standpoint of requiring justification for secrecy and confidentiality. Needless to say, our consultations with police and prosecutors have been very helpful in identifying legitimate law enforcement concerns and in balancing those concerns with the public's undoubted right to know how the scheme is functioning to the maximum extent which is compatible with such law enforcement objectives.

A review of the case-law surrounding Part IV.1 of the *Criminal Code* has helped to focus on areas of particular concern, areas where Part IV.1 has been difficult to apply, either because of a lack of clarity or direction in the legislation itself, or because the legislation is so different from other Anglo-Canadian legislation that police, lawyers and the judiciary have had difficulty interpreting and applying the provisions.

As a result of the consultation, other problems were brought to our attention, such as the interpretation and application of the legislation which, while never litigated, were sources of concern. We attempt to address those problems as well as we can in our discussions and recommendations.

IV. The Role of the Judiciary

Serious difficulties with the interpretation and application of Part IV.1 of the *Criminal Code* were perhaps to be expected, considering that the legislation is based on an American model. The legislation adopts exclusion of evidence as the fundamental sanction. This is not a regime with which Canadian courts are familiar. On the contrary, the general rule in the Canadian context, as expressed in *R.* v. *Wray*,[45] is that evidence is admissible no matter how obtained. The one exception to this rule relates to the admissibility of confessions, and bears no close analogy to exclusion of improperly obtained wiretap evidence. Moreover, derivative evidence from an improperly obtained confession is not subject to the exclusionary rule. The closest analogy to the wiretap regime is that of the search warrant, but at least prior to enactment of the *Canadian Charter of Rights and Freedoms*, it has been clear that improprieties in the obtaining or execution of a search warrant do not render inadmissible the fruits of the search.

45. *Supra*, note 8.

The situation since the enactment of the Charter may, of course, be different. At this stage, it would be wrong to attempt to foresee how the courts will deal with the exclusion of evidence under subsection 24(2) of the Charter in the case of an illegal search made pursuant to an improperly obtained search warrant. Certainly however, serious improprieties in the execution of a search warrant would likely render the evidence inadmissible.[46] It may well be that in the post-Charter era, the exclusion of evidence in the search warrant context will approach the position envisaged by the original wiretap legislation.

The reluctance of the common law to "police the police" through the mechanism of an exclusionary sanction has carried over into the interpretation and application of Part IV.1 of the *Code*. If the exclusion of evidence is to be an effective sanction, those circumstances in which evidence should be excluded must be identified with as much clarity as possible, as attempted in our recommendations.

The other theme which tends to be apparent is a reticence on the part of the judiciary, at the application stage, to see their role as one of supervising the exercise of police discretion. In view of the secrecy which surrounds the application process for authorization to intercept private communications, direct evidence of judicial reticence is not available. There is, however, circumstantial evidence in the statistics created pursuant to section 178.22 of the *Criminal Code*, and a review of those authorizations which, having been adduced at trials, are a matter of public record.

Again, the traditional role of the Canadian judiciary is not to become involved in the pretrial investigation. The one important exception, that of issuing search warrants, has a long history and, as the Commission's studies in that area have revealed, the degree of judicial control actually exercised is, at best, uneven.[47] Again, accepting Parliament's judgment that judicial control is necessary, it would seem to us that the circumstances in which authorizations should and should *not* be granted must be identified and spelled out, as must the contents of the authorization. In fact, the *Canadian Charter of Rights and Freedoms* would likely compel the conclusion that judicial control is appropriate. The legislation must recognize that it is essentially unfair to expect a judge, who is used to being the impartial arbiter, in effect to accept a supervisory role over the prosecution, without some very clear guidelines as to the limits of his authority. We feel that it is primarily up to Parliament, rather than the judiciary, to strike the balance between a justifiable intrusion and an unwarranted invasion of privacy, although obviously in the particular case the ultimate decision must be for the judge to make.

Although during the course of our consultations we encountered a spectrum of views concerning the degree to which the legislation should set out the criteria for granting the application, including terms or conditions, exclusion of evidence and so on, there was considerable consensus that the necessary flexibility could be accommodated within a statutory framework which would give more direction to the judiciary.

---

46. *R.* v. *Rao* (1984), 12 C.C.C. (3d) 97 (Ont. C.A.).

47. Law Reform Commission of Canada, *Police Powers — Search and Seizure in Criminal Law Enforcement*, [Working Paper 30] (Ottawa: Minister of Supply and Services Canada, 1983), p. 137 (hereinafter cited as the Search and Seizure Working Paper). Also see K.W. Lidstone, "Magistrates, the Police and Search Warrants," [1984] *Crim. L. Rev.* 449.

CHAPTER THREE

Our Recommendations and Commentary

This chapter of the Paper is structured so as to identify the problems, consider the options and make recommendations. It does not necessarily track the present legislation section by section. Rather, we have attempted to deal with areas of concern which often requires looking at several different sections. However, the present Part IV.1 of the *Criminal Code* must be seen as the background against which the recommendations would operate. Nevertheless, the relevant part of the present Part IV.1 is always referred to, if not quoted in full.

I. Application of Part IV.1 of the *Criminal Code*

A. The Offence

The principle of restraint would generally require that the investigative tool which is one of the most intrusive be resorted to only in the most serious cases or where it is most likely to produce results with a minimum of interference to legitimate privacy interests. *Code* section 178.1 presently defines "offence" by listing numerous offences under the *Criminal Code*, as well as some offences under other federal statutes, and incorporating a blanket provision relating to any other offence under the *Code* for which a maximum sentence of five years or more, or an offence mentioned in section 3 or 20 of the *Small Loans Act* "that there are reasonable and probable grounds to believe is part of a pattern of criminal activity planned and organized by a number of persons acting in concert; ...."[48] The importance of the law enforcement officers' need to use this type of tool was recognized, as members of organized crime and persons involved in very serious lucrative crime will use any equipment and techniques available to them.[49]

In the United States, at the time of adoption of Title III, organized crime was put forward as virtually the *raison d'être* for the legislation.[50]

48. *Criminal Code*, s. 178.1.

49. Canada, House of Commons, *Minutes of Proceedings of the Standing Committee on Justice and Legal Affairs*, June 5, 1972, Issue No. 13, p. 13:7.

50. American Bar Association, project on *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance* (Tentative Draft, June, 1968).

The ideal use of electronic surveillance to combat organized crime, it seems, would be as an intelligence-gathering mechanism. The ideal order, then, would tend to be person-oriented rather than offence-oriented, and would be of indefinite duration. On the other hand, there are serious problems with such a regime which were recognized at the time Part IV.1 was enacted. Perhaps the most obvious problem is that of satisfactorily defining "organized crime." The definition in *Code* section 178.1 is really little more than the definition of a conspiracy. Further, the Commission has rejected intrusions which perform a purely intelligence-gathering function, and has observed that "the general rule must be that intrusions upon these rights can only be justified following the initiation of an offence."[51] We consider this principle to be as applicable in the area of electronic surveillance as in the area of search and seizure. We are not persuaded that it is a principle which can be sacrificed on the basis of combating organized crime. We believe that the concerns as to the serious threat to life and property represented by organized crime and the difficulty of investigating that activity can be effectively met by a regime which is offence-specific and permits the granting of an authorization to investigate a conspiracy to commit such an offence (as does the present legislation).

Further, while some of the debate concerning Part IV.1 of the *Code* centred upon the utility of wiretapping as a means of combating organized crime, wiretapping has clearly not been limited to such activity. Thus, we think it inappropriate to design a wiretap regime premised on identifying offences committed by organized crime. We see no reason why trivial offences should fall within the wiretap regime because they may be committed by organized crime, nor do we see why serious crimes should be excluded because they are not traditionally committed by organized crime. We are also not convinced that the number of applications for a particular offence in the past is any measure of the need to include such an offence in Part IV.1. We accept, of course, that the large number of authorizations for certain offences is a measure of their utility in the investigation. On the other hand, the relatively small number of authorizations for investigating kidnappings or murders does not mean that, where appropriate, it is not vitally important that wiretapping be available to aid in the investigation.

While we see no alternative to listing offences, we think that it is possible, at the very least, to adopt criteria for including an offence in the list. In its *Fourth Report*, the Standing Committee on Justice and Legal Affairs proposed that the offence be a serious crime which threatens life, and individual and group well-being, to such an extent that the protection of privacy must yield to protection against antisocial activities.[52] The standard adopted by the American Bar Association in *Standards for Criminal Justice*[53] is that the offences be serious in themselves or characteristic of group activity. The advantage of the latter criterion is that it contains an element which focuses on the utility of wiretapping as an investigative tool. It seems reasonable that offences which are characteristic of group activity and thus require communication among participants, would likely be susceptible to wiretapping, and that wiretapping would produce

51. Search and Seizure Working Paper, *supra*, note 47, p. 137.

52. Canada, House of Commons, Standing Committee on Justice and Legal Affairs, *Fourth Report*, 1970.

53. American Bar Association, *Standards for Criminal Justice*, 2nd ed. (Boston: Little, Brown and Company, 1980).

significant quantities of evidence. In our view, the American Bar Association standard can be represented at the two extremes by murder as an offence which is serious in itself, and gambling as one characteristic of group activity. We think that both of these offences should properly be subject to wiretapping — murder because of its obvious seriousness, gambling because of the high degree of probability that *properly controlled* electronic surveillance would produce a high quality of evidence involving a minimum interference with legitimate privacy interests in circumstances where the offence would be otherwise difficult to detect. For both types of offences, the regime which we propose would attempt to ensure at the legislative level that there be a reasonable likelihood of useful evidence being obtained and, for the less serious offences, that the degree of intrusion be limited.

It has been argued that the definition of "offence" can be rationalized by simply permitting an authorization in the case of any indictable offence in the same way that a search warrant can be obtained in relation to *any* offence. We are not persuaded that such a rationalization is desirable or that the availability of a search warrant is the appropriate analogy in this regard. While the search of a person's home or office is certainly intrusive, it is qualitatively different from the intrusion contemplated by electronic surveillance. Even the most wide-scale search is an event lasting, at the longest, a day or two. It is directed towards uncovering existing evidence or contraband which there is a substantial likelihood not only exists, but exists in the place sought to be searched. Authorization of a wiretap, however, is predicated on the lack of existing evidence. It is not primarily directed at uncovering contraband or evidence, but is authorized in the expectation that evidence will be produced, not in the form of objects or documents but in the targets revealing their thoughts and ideas through communication. The search warrant analogy is valid only to the extent that it suggests the one parameter, namely that less "serious" offences should be targets of interception only where there is a substantial likelihood of uncovering evidence. The search warrant analogy is otherwise properly put in focus by considering whether a justice would knowingly authorize the daily search of premises for thirty to sixty days, the duration of most authorizations, no matter how serious the offence and how certain the prospect of obtaining evidence or contraband.

There is one other limited area which does not clearly fit into the dual standard, and that is offences which are integral to the wiretap regime itself, namely the offences created in *Criminal Code* sections 178.11 and 178.18. Our search of the annual reports made pursuant to section 178.22, which were available to us, has not turned up any resort to these provisions. On the other hand, inclusion of these offences in section 178.1 makes a statement about the commitment to privacy, since these offences really underlie the basic thrust of the legislation — namely, that unauthorized, nonconsensual wiretapping should be illegal.

Finally, we consider that the group activity criterion must be used with restraint. There should be a high degree of probability, from the nature of the offence, that evidence can only be obtained in this way. Further, offences which are not well defined in the *Code*, the investigation of which may infringe on fundamental values such as freedom of expression, should not be included in the list.

We recommend relatively minor changes to the present list of offences for which an authorization may be obtained. Our major recommendation, the elimination of the organized crime basis, was widely accepted, as most persons consulted agreed that it defied definition or proper application and was a potential source of abuse.

RECOMMENDATIONS

1. That the offences for which an authorization would be available continue to be listed. That the following offences be omitted from the present list in section 178.1: *Criminal Code* ss. 58 (forgery, etc.), 159 (obscene material), 195(1)(*a*) (procuring), 281.1 (advocating genocide), 314 (theft from mail), 331 (threatening letters, etc.), 339 (using mails to defraud); and *Excise Act*: ss. 158 and 163 (unlawful distillation or selling of spirits).

2. That the following *Criminal Code* offences be added to the list: ss. 195(1)(*b*), (*c*), (*d*), (*h*), and (*i*) (procuring, etc.), 305.1 (criminal interest rate),[54] 381.1 (threats to commit offences against internationally protected person).[55]

3. That the organized crime definition for offences be omitted but an authorization be available for investigation of: a conspiracy to commit; attempt to commit; being an accessory after the fact; and counselling, procuring or inciting in relation to any of the listed offences.

B. Private Communications

An essential aspect of the operation of a legislative scheme for the control of electronic surveillance is the decision as to which communications it is intended to protect. The definition of private communication recognizes that there is an inherent value in protecting privacy. While Part IV.1 of the *Code* contemplates (in paragraph 178.16(1)(*b*)) the use of evidence obtained as a result of unlawful interceptions if a

54. Addition of this offence perhaps requires some explanation. Deletion of the "organized crime" definition removes reference to the federal *Small Loans Act* (R.S.C. 1970, c. S-11). The intent of that reference was an attempt to deal with "loansharking," an offence often associated with "true" organized crime and with extortion. This area is now covered by the new *Criminal Code* section 305.1, and like extortion (section 305), it should be a targetable offence. It is an offence where the victim is particularly vulnerable and thus where effective enforcement may depend on the availability of evidence obtainable from the interception of communications.

55. Bill C-18, which was passed by Parliament, proposes in section 22, certain changes to *Code* section 178.1 which, in part, are similar to this recommendation. It does not eliminate any offences other than section 331 and paragraph 195(1)(*a*) (procuring) which however is replaced by a reference to "s. 195(1) (procuring)." As will be seen, we also recommend changes to section 195, but by replacing the reference to paragraph 195(1)(*a*) by a reference to other paragraphs which have the connotation of force and compulsion. Some of the offences in subsection 195(1) are simply not serious enough to warrant their inclusion.

party consents to the admission of the evidence, there is no question that the thrust of the legislation is to control the lawful use of electronic surveillance while criminalizing its unlawful use. " '[P]rivate communication' means any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it; ...."[56]

While it is only those activities in which a person has a reasonable expectation of privacy which require legislative control, the increasing use (real or perceived) of electronic surveillance by state agencies has led to the uncomfortable prospect that it is not unreasonable for persons to suspect that their telephone lines are tapped. If such a trend were to continue, then wiretapping could become uncontrolled, the authorities relying on the societal reasonable apprehension as to the widespread use of wiretapping equipment.[57] This view was expressed by Mr. Justice Brooke, in a recent decision of the Ontario Court of Appeal,[58] who observed that where there was evidence that the respondent knew there was a real danger his telephone communications would be intercepted, it was questionable whether it could properly be said that these communications were made under circumstances in which it was reasonable to expect that they would not be intercepted by any person other than the person whom he intended to receive it.

This displays a certain insensitivity to the purposes behind the enactment of Part IV.1 of the *Code*. Leaving aside "criminals," many innocent persons have nagging fears which could express themselves in similar kinds of utterances to the effect that their telephones are being wiretapped. Writing in 1974, Professor Amsterdam, in another context, focused on the problem of tying regulation of invasions of privacy to the person's subjective reasonable (rather than justifiable) expectation of privacy. He concluded that an "actual, subjective expectation of privacy obviously has no place in ... a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection."[59]

The public's legitimate interest in the protection of privacy could be seriously undermined if the definition of "private communication" is not adjusted. A new definition would have to take into account the fact that knowledge as to the existence of wiretapping is becoming more prevalent, while making it clear that a party to a "private" communication still has a "reasonable" expectation of privacy where his only concern centres on the possibility of lawfully authorized interceptions.

Another problem identified in the definition of "private communication" was discussed in the decision of the Supreme Court of Canada in *Goldman* v. *The Queen*.[60] In that case, it was argued that the communications which had been intercepted by

56. *Criminal Code*, s. 178.1.

57. *R.* v. *Carothers*, [1978] 6 W.W.R. 571 (B.C. Co.Ct.).

58. *R.* v. *Samson* (1983), 9 C.C.C. (2d) 194 (Ont. C.A.), p. 204.

59. Amsterdam, *supra*, note 40, p. 384.

60. *Supra*, note 33.

means of a "body pack" (a radio transmitter worn by the person) were not private communications because the police agent as the "originator" knew of the interception. McIntyre J. resolved the issue in a pragmatic way by holding that the "originator" is the person "who makes the remark or series of remarks which the Crown seeks to adduce in evidence" on the theory that:

> [W]here a police officer or police agent participates in a conversation with a suspect knowing that it is being intercepted electronically and hears the suspect make hoped for inculpatory statements of importance to the Crown's case, I am unable to consider the police officer to be the originator of the very statement or statements he was seeking to obtain.[61]

Without in any way minimizing the difficulty of the problem of interpretation dealt with by the court, we do not believe that it is immediately apparent that the policy of the legislation favours the interpretation adopted by the court. To take the *Goldman* case itself, the only difference between Part IV.1 applying or not, was that additional procedural hurdles had to be overcome to admit the tape of the conversation, than would have been necessary had the police agent been available and able to testify as to his personal recollection of the contents of the conversation. The *privacy* interest in the *Goldman* case is highly abstract in such circumstances. The primary issue is not one of electronic surveillance. That is only incidental to the broader question of the use of police agents. The only genuine justification for the application of Part IV.1 to the *Goldman* situation is that of discovery, namely, making the notice provisions of *Code* subsection 178.16(4) applicable. While there is a policy component, it should be one which encourages compliance with the authorization procedure in situations involving true privacy interests, and which is at the same time a rule that can be applied practically. Even the *Goldman* rule suffers on this latter account since it calls for the court to break up a conversation into separate "communications." In our view, Part IV.1 should protect the privacy of conversations, not individual communications. The overriding policy must be one which favours a simple, practical and easily applied rule. The easiest solution is to define "private communication" to include the entire conversation in which either of the parties has an expectation of privacy. The bodypack problem can be dealt with separately with respect to the admissibility and offence-creating sections.

We were, however, concerned that this new definition could pose problems in two areas: prisons and other lock-ups; and, hostage-taking situations. Under the present legislation, where the hostage taking is a public event with the culprits using the telephone to negotiate with the police or to talk to others, it would not seem that a new definition would pose any problems. It would be unreasonable on anyone's part to believe that such communications were not being monitored;[62] yet that belief may stem from a belief that the monitoring was being done by a court-ordered authorization. The issue is this: Do hostage-taking incidents present such a serious and immediate threat to the lives and safety of others that a special exemption should be built into the proposed definition of "private communication"? If so, then the police would be at liberty to

---

61. *Id.*, p. 995 (S.C.R.), p. 16 (C.C.C.).

62. See *R.* v. *Gamble and Nichols* (1978), 40 C.C.C. (2d) 415 (Alta. S.C. A.D.), p. 424.

intercept communications in such circumstances without a court authorization. In our view, in such public hostage-taking incidents, the privacy interest is extremely attenuated, while the risk of danger to persons is so extreme that the law must be carefully drafted to ensure that, as before, the public hostage taker's communications with the outside are not "private communications." We believe that Recommendation 4 accomplishes that purpose.

The other problem concerns prison communications. As a matter of security, the communications of inmates with the outside world are monitored by the institution staff. One method of legitimating this process is to post signs on the institution telephones to the effect that the conversation is being or may be intercepted.[63] Under the current definition, such interceptions would not be of private communications, would thus be outside the provision of Part IV.1 and, would therefore not be unlawful. Under our proposed definition, the interception would still be of a private communication, since the party outside the prison might reasonably believe there was no interception. Approached in this manner, the problem is solved not by distorting the definition of "private communication" but by making such interceptions lawful, through an amendment to section 178.11.

There is some controversy as to whether Part IV.1 applies to eavesdropping without the use of electronic devices. In *R.* v. *Beckner*,[64] the court held that Part IV.1 did not apply. However, in the earlier decision in *R.* v. *Boutilier and Melnick*,[65] the contrary result was reached. In our view, the conclusion reached in *Beckner* is correct. While the need to regulate all police intrusions into privacy can be argued, at some point there is a *de minimus* quality to the debate. The corner-stone of any privacy regime is what it outlaws as much as what it permits. To require regulation as to the admissibility of overheard conversations implies the outlawing of such conduct, except in specified circumstances. This would require a radical change in the way most people conduct themselves, even in commonplace everyday activities.[66]

A related problem is a highly technical one arising from the inclusion of "telecommunication" in the definition of "private communications." "Telecommunication" is defined in section 28 of the *Interpretation Act* as meaning "... any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system; ...."

The same definition is also used in *Criminal Code* sections 287 (theft of telecommunication service) and 287.1 (possession of device to obtain telecommunication facility or service). That definition is very wide, and questions have been raised as to whether it would cover the interception of communications transmitted to such things as paying devices which are capable of being private communications within the definition.

---

63. See *R.* v. *Rodney* (1984), 12 C.C.C. (3d) 195 (B.C. S.C.).
64. *R.* v. *Beckner* (1978), 43 C.C.C. (2d) 356 (Ont. C.A.).
65. *R.* v. *Boutilier and Melnick* (1976), 35 C.C.C. (2d) 555 (N.S. S.C.).
66. See *supra*, note 4, p. 44.

However, the definition might also cover the use of devices sometimes referred to as pen registers which do not acquire any conversation, only the numbers dialed from the telephone. The consensus among law enforcement authorities is that these devices are not covered by the legislation and should be available without having to resort to the authorization procedure. In fact, such a device might be used in preparation of the material to obtain an authorization by assisting to track the members of the alleged conspiracy. It is clear that such devices are not covered by the United States legislation, Title III,[67] which refers only to "aural" interception of private communications. Warrantless use of such devices also does not violate the Fourth Amendment on the theory that a person does not have a reasonable expectation of privacy concerning the numbers dialed.[68] It is our view that there is no reasonable basis for inclusion of the pen register and related devices (such as diode devices used to track the number of an incoming call after the caller has hung up) within the Part IV.1 legislative scheme. Part IV.1 is primarily directed at protecting privacy of communications; that is, discourse between persons. These devices do not invade the privacy of the communication. Moreover, the expectation of privacy in telephone numbers called or received is minimal. To clarify the law in this respect, the proper remedy is a slight adjustment of the definition of "electromagnetic, acoustic, mechanical or other device."

RECOMMENDATIONS

4. That "private communications" be defined as follows:

any oral communication or any telecommunication made under circumstances in which it is reasonable for any party to it to expect that it will not be intercepted by any electromagnetic, acoustic, mechanical or other device.

5. That a communication does not cease to be a private communication only by reason of a belief on the part of a party to it that the communication may be the subject of an authorization obtained from a court by a law enforcement agency.

6. That subsection 178.11(2) be amended by the addition of paragraph (*e*) as follows:

a person engaged in monitoring for security purposes of communications of inmates of a prison as defined by the *Prisons and Reformatories Act*, R.S.C. 1970, c. P-21, and a penitentiary as defined by the *Penitentiary Act*, R.S.C. 1970, c. P-6, where the fact that such monitoring may occur is prominently displayed at the place where the communication may occur.

---

67. *U.S., Omnibus Crime Control and Safe Streets Act of 1968*, Title III, Act of June 19, 1968, Pub. L. No. 90-351 (hereinafter cited as Title III). See also J.G. Carr, *The Law of Electronic Surveillance* (New York: Clark Boardman, 1977), p. 74.

68. *Smith* v. *Maryland*, 442 U.S. 735 (1979). However, see, *People* v. *Sporleder*, 666 P.2d 135 (Colo. 1983).

7. That the definition of "electromagnetic, acoustic, mechanical or other device" be amended as follows:

> **"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used, or is capable of being used, to intercept a private communication, but does not include a hearing-aid used to correct subnormal hearing of the user to not better than normal hearing, nor a device such as a pen register, touch-tone decoder, diode device or other similar device used to acquire the identity of the telephone number dialed, or of the caller, the time and the date of the telephone call, but which is not capable of intercepting any words or other information.**

C. Optical Devices

Closely allied to the definition of "private communications" just discussed, and hence the application of Part IV.1, is the problem of the use of optical devices.

It seems clear that the present Part IV.1 does not cover optical devices.[69] In its 1980 discussion paper, the Australian Law Reform Commission identified the use of optical devices as a serious privacy problem (in contrast to the position taken in its Report on *Criminal Investigation*[70]). "In the past simple safeguards could normally be taken by people to secure their privacy against unwanted observation by uninvited third parties. Today, those safeguards are inadequate. Advances in technology have not been confined to listening and interception devices."[71]

While we can appreciate the *potential* for serious privacy issues to arise in the area, there is little evidence at present that the use of optical devices has led to serious abuse or problems of unjustifiable intrusion into privacy. To attempt to legislate in a broad manner in this area would involve serious infringements on the rights of property owners. One cannot legitimately prevent the owners of property such as banks, convenience stores, and so forth from installing cameras to protect the premises from illegal conduct. Another use made of such devices is to record illegal transactions between suspects and police agents. Like the use of body packs, this use of optical devices raises only very theoretical privacy issues. Finally, there is the use of devices such as binoculars and telescopes. The United States Supreme Court has considered this issue in relation to the Fourth Amendment protection against unreasonable search and seizure. In *United States* v. *Knotts*,[72] the court, considering the implications of the use of a

69. *R.* v. *Biasi (No. 3)* (1981), 66 C.C.C. (2d) 566 (B.C. S.C.).

70. Law Reform Commission of Australia, *Criminal Investigation*, [Report No. 2] (Canberra: Australian Government Publishing Service, 1975).

71. *Supra*, note 4, pp. 64-5.

72. *United States* v. *Knotts*, 103 S.Ct. 1081 (1983).

beeper which transmitted an electronic signal permitting officers to monitor the location of the suspect's vehicle, observed that "nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[73]

Without a great deal more research on the types of devices presently in use and their capabilities, we do not believe that it is possible to legislate in this area in a comprehensive way. It is, however, possible to identify one narrow area where the issues are clear and the privacy interest high, that is, the surreptitious entry of private premises by governmental officials to install optical devices. We propose to regulate such conduct in the same manner as surreptitious entry to install listening devices ("room bugs"), and to leave the other questions for further study. We simply do not feel confident in addressing all the competing policy issues which may arise by adopting a broader test such as regulation of devices in every place where a person has a reasonable expectation of privacy.

Moreover, because we intend to regulate surreptitious entry for installation of listening devices, to leave the area of optical devices unregulated would leave a gap which could permit persons, including law enforcement authorities, to do indirectly what the law otherwise prohibits.

In leaving this subject we wish to make clear that we do not in any way minimize the problems created by law enforcement use of optical devices, even with the consent of the property owner. Whether or not this is an appropriate use of resources, we do not feel that it is an area upon which we can make any recommendation, other than to suggest that the entire field of surreptitious optical surveillance requires study.[74]

RECOMMENDATIONS

8. That it be an offence to enter private property without a court order or the consent of the owner or lawful occupier for the purpose of installing an optical device.

9. That an authorization to install an optical device be available by application to a court, but only under the same conditions as an authorization is available for installation, by surreptitious entry, of a listening device.

10. That "optical device" be defined for the present time as any electronic device or mechanism capable of permitting surreptitious viewing of persons or things.

---

73. *Id.*, p. 1086. On the other hand, electronic devices such as a beeper cannot be used to obtain information which would not have been open to visual surveillance, such as a private residence (see *United States* v. *Karo*, 104 S.Ct. 3296 (1984)), notwithstanding that the beeper is less intrusive than a full-scale search.

74. See *U.S.* v. *Torres*, 36 Cr.L. 2301 (December 19, 1984) (7th Cir.), p. 2302.

D. Foreign Interceptions

Another problem which exists with the application of Part IV.1 of the *Criminal Code* is that of interceptions made in foreign countries.

Several recent court decisions in British Columbia have raised the problem of regulation of evidence gathered as the result of an interception made in a foreign jurisdiction. This is an evidentiary problem, since it is conceded that Canadian substantive law can have no reach into other countries so as to attempt to regulate conversations taking place wholly in such countries. Opposing decisions of the British Columbia Supreme Court have held, on the one hand, that the foreign interceptions are inadmissible unless proved to have been lawfully intercepted according to the law of the foreign jurisdiction,[75] and on the other hand, that Part IV.1 did not apply to such interceptions, and admissibility was therefore governed by the general law of evidence.[76] A third option would be to require the interception to conform to Canadian standards. It should be pointed out that this could lead to exclusion of evidence from many countries such as Great Britain[77] where wiretapping is authorized by the Home Secretary rather than by a judge. Neither the application of the principles of criminal procedure nor the interest in protection of privacy immediately identifies the optimal option, or the solution. Canadians who choose to conduct business outside Canada must expect to have that business regulated by foreign governments, and perhaps to have their privacy invaded at the whim of that government.

Other relevant principles are respect for international obligation, economy, clarity and fair and efficient administration of justice. In our view, it would be highly impracticable and disrespectful of international obligations to impose the Canadian regime on foreign governments (the third option).

The one argument presented in favour of the third option is that since the accused is being tried in Canadian courts according to Canadian due process, the evidence presented must accord with Canadian standards of admissibility. The argument is analogous to the confession rule. For example, just as Canadian courts would not accept a confession obtained by torture, even assuming that such activities were lawful in the state where the confession was obtained, so too we should not accept that state's rules in other circumstances. When the accused is tried in Canada, the Canadian rules of procedure must be considered the minimum. Inequality of treatment could arise. Two accused tried in Canada may have had their conversations intercepted, one in Canada, one in the foreign state but by the same means. In the one case, the interception not having been in accordance with Part IV.1, the evidence would be inadmissible. In the other case, the interception, having conformed to the foreign state's lower requirements, would be admissible.

---

75. See: *R.* v. *Bengert (No. 8)* (1979), 15 C.R. (3d) 37 (B.C. S.C.); *R.* v. *Bengert (No. 9)* (1979), 10 B.C.L.R. 199, 15 C.R. (3d) 40 (B.C. S.C.).

76. *R.* v. *Newall (No. 1)* (1982), 67 C.C.C. (2d) 431, 136 D.L.R. (3d) 734 (B.C. S.C.).

77. See *Malone* v. *Commissioner of Police of the Metropolis (No. 2)*, [1979] 2 All E.R. 620; 69 Cr. App. R. 168 (Ch.D.).

We are not convinced that the logic of these arguments is so compelling as to require the adoption of this third option.

The confession analogy does not really provide a principled basis in the wiretap area. In the first place, confessions are excluded unless voluntarily obtained: (a) to ensure their trustworthiness; and (b) to vindicate the principle against self-incrimination.[78] Neither reason applies to wiretap evidence no matter how obtained. Trustworthiness, in particular, turns on the reliability of the interceptors, not the quality of the legislative scheme which gives them the right to intercept. Further, except for the confession rule, the law in Canada prior to the Charter was that evidence, no matter how obtained, was admissible. Evidence has been used in Canadian and other common law courts, which has been obtained in violation of a host of common law and statutory rights and even in violation of the confession rule[79] without any compunction.

The only due process component upon which Canada can legitimately insist in this area is that resort to the foreign interception was not done in bad faith to avoid the Canadian requirements.

On this question, it would be useful to consider the United States experience, much of which has in fact involved admissibility of communications intercepted by Canadian authorities before and after passage of Part IV.1. Those authorities clearly hold that where the interception was not unlawful under Canadian law (even prior to passage of Part IV.1) the evidence is admissible in United States courts outside of Title III.[80] The authorities, however, are not entirely clear as to the effect of an illegal interception (that is, illegal under the laws of Canada). It seems to depend on the perspective from which the court approaches the question. In *United States* v. *Maher*,[81] the court approached the question from the perspective of the principle underlying the domestic exclusionary rule.

In *United States* v. *Phillips*[82] the court took a broader approach from the perspective that international comity was the principle involved, and it excluded evidence obtained from illegal interceptions (that is, illegal under Canadian law).

Either of these approaches can be defended, depending on the choice of the paramount principle. The approach in *Maher* in particular, which requires domestic connivance, seems suited to the Canadian context. A test for admissibility, which has about

78. *Rothman* v. *The Queen* (1981), 59 C.C.C. (2d) 30 (S.C.C.), *per* Lamer J., p. 63.

79. *R.* v. *St. Lawrence* (1949), 93 C.C.C. 376 (Ont. H.C.J.).

80. *United States* v. *Cotroni*, 527 F.2d 708 (1975), (2d Cir.) cert. den. 426 U.S. 906 (1975); *Stowe* v. *Devoy*, 588 F.2d 336 (1978), (2d Cir.) cert. den. 442 U.S. 931 (1978).

81. *United States* v. *Maher*, 645 F.2d 708 (1981), (9th Cir.), pp. 782-3.

82. *United States* v. *Phillips*, 479 F.Supp. 423 (1979) (M.D. F.C.), pp. 437-8.

it an element of shocking the conscience, is reminiscent of subsection 24(2) of the Charter. It is to be noted that, even under the *Phillips* test, it would appear to place the burden on the accused to demonstrate the illegality under the foreign law.[83]

Accordingly, one solution would be to provide that Part IV.1 applies to foreign interceptions only to a very limited extent. Since the interception takes place outside Canada as explained above, the privacy interest is not paramount. Rather, the paramount principle is concern for vindication of the process itself as indicated by Mr. Justice Lamer in *Rothman* v. *The Queen*,[84] who identified this value when considering the admissibility of a confession obtained by a trick.

Similarly, a blatant disregard for the procedure established in Canada to control interception of private communications ought not to be countenanced. In *Rothman*, Lamer J. considered the appropriate method of control as exclusion of evidence where, by reason of the conduct of persons in authority, to admit the evidence would bring the administration of justice into disrepute. Such a test is similar to the exclusionary rule in subsection 24(2) of the *Canadian Charter of Rights and Freedoms*, although Lamer J. adopted a rigorous test requiring that the conduct

> must be so shocking as to justify the judicial branch of the criminal justice system in feeling that, short of disassociating itself from such conduct through rejection of the statement, its reputation and, as a result, that of the whole criminal justice system, would be brought into disrepute.[85]

It seems unlikely that such a rigorous test would apply under subsection 24(2) of the Charter[86] and we have considered leaving the admissibility of evidence obtained by a foreign interception to be determined by resort to subsection 24(2) of the Charter. However, this could lead to an undesirable uncertainty in the law since it is not at all clear whether conduct by officials outside Canada would constitute violations of a person's rights, a necessary pre-condition to invoking section 24(2), under the Charter. Accordingly, we have opted for a clear but narrow rule focusing directly on what we see as the legitimate Canadian interest, namely protection of the integrity of the system.

We have, moreover, opted to put the initial evidential burden of proof on the accused which, when satisfied, activates the Crown's persuasion burden. We recognize that the practicalities of the matter are that, in most cases, this will effectively preclude investigation of the manner in which the foreign interception was conducted, but we can see no viable alternative.

Finally, we believe foreign interceptions should otherwise be integrated into the regime insofar as notice of introduction into evidence is concerned.

---

83. In *Phillips* that was not difficult, since the case arose out of the Royal American Shows investigation, and there was Canadian judicial authority on the very issue.

84. *Supra*, note 78, p. 72.

85. *Id.*, p. 74.

86. See *R.* v. *Simmons* (1984), 11 C.C.C. (3d) 193 (Ont. C.A.).

RECOMMENDATIONS

11. That primary and derivative evidence obtained from an interception made outside Canada, no matter where the private communication originated, be admissible in evidence whether or not the interception was lawfully made, provided that the interception was not made in the foreign jurisdiction in violation of the laws of the jurisdiction with the connivance of Canadian authorities.

12. That the court before which evidence from a foreign interception is tendered shall conduct an inquiry into the admissibility of that evidence only where the person against whom the evidence is sought to be admitted leads some evidence from which the court could find that the interception was made in violation of the laws of the foreign jurisdiction with the connivance of Canadian authorities.

13. That the notice provisions in present *Code* subsection 178.16(4) apply to evidence obtained from foreign interceptions.

E. Participant Monitoring: Consent Interceptions

Another issue is the question of consent interceptions, made without judicial authorization because a party to the "private" communication agrees to the interception.

Paragraph 178.11(2)(*a*) exempts consent interceptions from the scope of the legislation. This embraces two situations: (1) where one of the participants to the conversation, with or without the knowledge of the other(s), himself tape-records the communication; and (2) a third party with the consent of one of the participants intercepts and records the communication. In view of the *Goldman* v. *The Queen*[87] formulation of "private communications," both these situations embrace private communications at least where the evidence is offered against the nonconsenting party, but in both situations the recording and interception are lawfully made, and evidence so obtained is admissible in evidence *per* paragraph 178.16(1)(*a*). It is the scheme of the legislation that no prior judicial authorization is required.

The Supreme Court of Canada, in *Goldman* v. *The Queen*, indicated that a consent under paragraph 178.11(2)(*a*) is valid and effective "if it is the conscious act of the consentor doing what he intends to do for reasons which he considers sufficient." The consent must be "one he intended to give and if he gives it as a result of his own decision and not under external coercion the fact that his motives for so doing are selfish and even reprehensible by certain standards will not vitiate it." Further, the consent must not be procured by intimidating conduct, force or threats of force by the police, but coercion "does not arise merely because the consent is given because of promised or expected leniency or immunity from prosecution."[88]

87. *Supra*, note 33.

88. *Id.*, p. 1005-6 (S.C.R.), p. 24 (C.C.C.).

This formulation was subjected to some criticism in Working Paper 30, at least at it might apply to search and seizure.[89] We do not think, however, that such a criticism is as valid in the area of consent interceptions. Unlike a "consent" search, a consent interception not only usually involves passive consent but also the active participation of the party.

The most common usage of consent interceptions in the law enforcement context is the recording of a conversation between the suspect and a police agent or an undercover police officer. However, consent recording takes place in many other contexts. Businessmen, for example, may routinely record their own telephone calls or their own meetings. Such a practice is not generally perceived to be illegal.

Concerns have been expressed to the Commission about the desirability of continuing the current system whereby consent interceptions are outside federal control. It may be that even in official use, such interceptions are far more frequent and persuasive than the court-authorized procedure.[90] The concerns have been expressed on two levels, (1) privacy and (2) evidentiary. The privacy concern focuses on the fact that widespread consent recording can, in the long run, compromise the free flow of ideas and affect free speech in an undesirable way. If persons may come to believe that their conversations are being recorded, they will be less candid for fear that their words may come back to haunt them.

The evidentiary concern focuses on the possibility of manipulation by the party who knows of the interception. The knowing party can direct the conversation not only to draw out the suspect and make him incriminate himself, but at the same time may shield his own involvement and produce self-serving evidence. Further, the simple introduction of the tape recording can be misleading to the trier of fact unaware of the effect of the psychology of the situation.

Proposals offered for reform of the law in this area are: first, to continue to provide that consent interception be lawful but not to permit the recording to be introduced into evidence; and second, to bring consent interceptions into line with the rest of the legislative scheme and to require prior judicial approval — the interception, even with consent, would be otherwise unlawful, and the evidence would be subject to exclusion in the same way as other evidence which is the product of the unlawful interception.

We believe that neither proposal is acceptable, and that the law must be maintained essentially as it is now. We have been influenced in this respect by the Australian Law Reform Commission. Although the Commission had, in an earlier paper, suggested adopting a warrant requirement, in its 1983 report on *Privacy*[91] the Commission rejected

89. Search and Seizure Working Paper, *supra*, note 47, pp. 162-3.

90. J.G. Carr, "Electronic Surveillance by Consent under State Law" (November, 1984), 11 *Search and Seizure Law Report* 77.

91. Law Reform Commission of Australia, *Privacy*, [Report No. 22] (Canberra: Australian Government Publishing Service, 1983) (2 volumes).

this view. The reasons given are cogent and equally applicable in the Canadian context (if not more so, considering the ten-year history of legalized consent interceptions). The majority of the Commission stated as follows:

> 1131. *Dangers of Regulating Participant Monitoring*. There are a number of dangers with proposals that participant monitoring, generally, be prohibited. Tape recording of sounds and conversations is now a common practice in purely domestic and friendly circumstances. Tape recordings can be taken of family events, without someone there being aware that it is happening. It can be done at parties for fun. This conduct should not bear the full weight of the criminal law. Accidental recording without the consent of some parties might also occur. The innocent recorder of social events might be placed at a risk completely disproportionate to the undesirability of what he may have done.
>
> 1132. *Fundamental Problem Unresolved*. A person speaking to another does so at his own risk. Whatever he says can be recalled, correctly or incorrectly, by the other parties to the conversation and can be reported, correctly or incorrectly, as they see fit. A person speaking to another must take the risk, ordinarily inherent in so doing, that his hearer will make public what he has heard. There are many ways of recording conversations. Notes written immediately after the conversation has finished is one way. Shorthand notes, or longhand notes, taken during the conversation are others. A listening device simply replaces other techniques of recording that the party to the conversation might use. The fundamental difficulty — the fact that the conversation can be recorded or recalled in circumstances and for purposes outside one party's control — still remains. To regulate the use of some forms of recording does not remove that difficulty.[92]

The first proposal, that is, prohibiting admission of evidence, seems undesirable. Expert evidence, as to the distortion of the nature of the conversation in favour of the knowledgeable participant, can well be called at the trial, just as linguistic evidence has lately been adduced in several trials in an effort to diminish the weight which the trier of fact should attach to a confession.[93] We think it would be wrong, however, as a general rule to exclude evidence which may be highly cogent and of great assistance to the trier of fact. Consider the following problems: Could defence counsel cross-examine a witness (say, a police informer) on a transcript of a recorded conversation to impugn his recollection of the conversation? Would the accused be barred from introducing a tape recording of a conversation with another person which could raise a doubt as to the accused's own guilt? If the accused denies that any conversation took place as alleged by the police agent, would the Crown be barred from leading a tape recording of that conversation? We believe that any attempt to regulate consent interceptions would be introducing an unnecessary complexity without any real gains in terms of accuracy of fact-finding or protection of legitimate privacy interests.

It should be noted that because of the recommended alteration to the definition of "private communications" it is necessary to expand the exceptions to the offences in *Code* subsection 178.18(1). That section makes it an offence to be in possession of a device knowing that the design thereof renders it primarily useful for "surreptitious

92. *Id.*, vol. 1, paras. 1131-2, p. 49.

93. See: *R.* v. *Lapointe and Sicotte* (1983), 9 C.C.C. (3d) 366 (Ont. C.A.); *R.* v. *Lessard* (1982), 10 C.C.C. (3d) 61 (Qué. C.A.).

interception of private communications." Under the *Goldman*[94] formulation, one could never be sure until after the fact whether the communications being tape-recorded by a party to it were private communications, since whether or not a communication was a private communication depended on who the originator was.

Under our proposals, even where one party consents to, or in fact makes, the tape recording (interception), the communication is private if another party to it has a reasonable expectation of privacy. Accordingly, persons in possession of tape recorders designed to record their own conversations without the knowledge of the party could now find themselves liable criminally, depending on the meaning to be attached to the word "surreptitious." We therefore propose an amendment to section 178.18 to clarify that an interception in such circumstances is not unlawful. This would also alleviate the necessity for the proposed amendment in section 25 of Bill C-18 to *Code* section 178.18.[95]

RECOMMENDATIONS

14. That section 178.11 continue to provide that it is not unlawful to intercept private communications where the interception is made with the consent, express or implied, of any party to it.

15. That the offence in subsection 178.18(1) not apply to any person in possession of a device or component for the purpose of using it in an interception made or to be made with the consent of one of the parties.

16. (1) That a peace officer, before commencing an interception under this section, shall inform the person whose consent is sought that he has a right to refuse to consent and to withdraw his consent at any time.

(2) That consent under this section may be given orally or in writing.

17. That the signature of a person on a document warning him of his right to refuse to consent and of his right to withdraw his consent at any time or a recording of such consent be *prima facie* proof of the consent of the person to the interception.

---

94. *Supra*, note 33.

95. That amendment would add to the list of exemptions from liability paragraph 178.18(2)(*b*.1) as follows:
... a person in possession of such a device or component under the direction of a police officer or police constable in order to assist that officer or constable in the course of his duties as a police officer or police constable: ....

II. The Authorization

A. The Application Procedure

Section 178.12 of the *Criminal Code* provides that the application for an authorization is to be made *ex parte* by a designated agent to a Supreme Court judge or a judge as defined by *Code* section 482 which, in provinces which have them, includes a judge of the county or district court. In Québec, the effect of reference to section 482 is also to include provincial court judges. Concern has been expressed that the application is *ex parte*, the only persons present being the judge, the agent and the police officer who swore the affidavit which, pursuant to subsection 178.12(1), must accompany the application. While a similar concern could be raised with respect to the ordinary search warrant procedure, the Supreme Court of Canada has held that such a proceeding may be *in camera*.[96]

It would, of course, defeat the purpose of the application if the proposed target were given notice of the application, but suggestions have been made for the assignment of *amicus curiae* or *amicus publicae* to represent, in a sense, the interests of the proposed target, and presumably the public interest to some extent as well. Cohen has observed that "[s]ecrecy could still be maintained, but the public would gain a measure of added assurance that the privacy interest was receiving more than simple lip-service."[97] The idea of an *amicus publicae* has received little support and, while the concerns which Cohen and others have raised cannot be dismissed, we are not prepared to recommend the establishment of such an institution, provided that our recommendations concerning disclosure of the material used on the application are implemented. Since in the end the *amicus* would be dependent upon the authorities for his information, it is not clear that such an institution would afford a significant or real protection to privacy. We would be concerned that the *amicus* would afford only the illusion of protection and would undermine arguments in favour of implementing the disclosure recommendations which we believe have the potential to afford real protection and accountability.

At present, the *ex parte* hearing is not only *in camera*, but is also not transcribed. There is no court reporter present and no recording is made. Some uncertainty exists as to whether the judge may question the affiant and supplement, by oral testimony, the facts in the affidavit. It has been pointed out that on the renewal application, in addition to the written application and the affidavit, the application may be supported "by such other information as the judge may require." Again, it is not clear in what form this information should be received. This uncertainty can have serious consequences if the recommendations with respect to disclosure are adopted, since the application procedure will be more open, and hence, more open to challenge. While the

96. *Attorney-General of Nova Scotia* v. *MacIntyre*, [1982] 1 S.C.R. 175, 65 C.C.C. (2d) 129.
97. Stanley A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (Toronto: Carswell, 1983), p. 137.

authorizing judges should be encouraged to challenge the material in the affidavit, there must be a record of any statements from the officer which are relied upon to grant the authorization so that they are available when there is a later review. Accordingly, we adopt the same procedure recommended in Working Paper 30 with respect to search and seizure.[98]

RECOMMENDATION

18. That the application for an authorization or renewal continue to be in writing and accompanied by an affidavit of a peace officer. The hearing shall be *ex parte* and *in camera*. The judge should be empowered to place the peace officer under oath to ascertain additional facts underlying the application. However, if such facts are relied upon in the adjudication of the application, a record of such facts shall be included in the sealed packet.

B. Basis for Granting the Authorization

The basis upon which an authorization may be granted is set out in *Code* subsection 178.13(1) and is intended to emphasize the extraordinary nature of the intrusion. The core of the limitation is contained in paragraph (*b*) which requires that the judge be satisfied:

> ... that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

While to a certain extent this implements the "last resort" criteria which properly attend the use of this method of investigation, it does not address the more nebulous problem of the gravity of the suspected offence. As indicated above, while electronic surveillance was seen as a necessary tool to fight organized crime and other serious crime, in practice its use has never been so restricted. Throughout our consultations, concerns were voiced that electronic surveillance was being misused in the investigation of trivial offences. While we have not cut back significantly on the authorizable offences listed in section 178.1, we still consider that the public interest is best served by the restriction of so intrusive an investigative tool to serious examples of the authorizable offences. Accordingly, we propose amendment to paragraph 178.13(1)(*a*) which presently provides that the judge be satisfied:

> that it would be in the best interest of the administration of justice to do so; ....

98. *Supra*, note 47, pp. 185-8.

RECOMMENDATION

19. That paragraph 178.13(1)(*a*) be amended to provide that the judge may grant an authorization where he is satisfied that it would be in the best interest of the administration of justice and in the public interest having regard to the seriousness of the offence under investigation.

C. Interprovincial Offences

Organized crime and other types of crime do not necessarily respect provincial boundaries. The issue has been raised whether judges in one province have jurisdiction to authorize an interception in another province. To date, the answer seems to be in the negative[99] although in *R.* v. *Bengert*,[100] Berger J. held that the Superior Court could authorize interceptions outside the province. Our view is that, at present, Part IV.1 does not permit such authorizations. Moreover, Osler J. pointed out in *Re Application for Authorization to Intercept Private Communications*, that what is "normally authorized and the conditions under which the authorization may be exercised, may vary considerably from province to province."[101]

Several solutions have been proposed for this problem:

(a) "Backing system" similar to the procedure in *Code* subsection 443(2).

While this solution was favoured by several government representatives, we see serious problems. For example, on what material would the "backing" judge act? Should he review the initial application, or merely rubber-stamp the authorization? What criteria would govern the exercise of his discretion? And what of the police? If the authorization is backed, would they be required to implement the order and perhaps commit scarce resources to a project to which they would ordinarily give a low priority? At the very least, the application to back the authorization would have to be accompanied by an affidavit of a peace officer in the judge's jurisdiction indicating willingness to carry out the order and further indicating that the application has been approved by an agent of the provincial Attorney General or the Solicitor General as the case may be.

(b) Amendment of section 178.13 to give the judge the power to authorize an interception in another province.

We think that the issues raised by Osler J. and set out above, are the appropriate considerations and that this would not be the proper solution.

---

99. *Supra*, note 76, *per* Bouck J.; and *Re Application for Authorization to Intercept Private Communications* (1983), 9 C.C.C. (3d) 347 (Ont. H.C.J.), *per* Osler J.

100. *R.* v. *Bengert*, [1979] 1 W.W.R. 193 (B.C. S.C.).

101. *Supra*, note 99, p. 349.

(c) Amendment of section 178.13 to give the judge of the Federal Court power to authorize interception anywhere in Canada.

This is not a solution which has found favour with any of the persons consulted. Apart altogether from any other concerns, judges of the Federal Court have not previously been involved with electronic surveillance applications under Part IV.1 and have not been able to develop the necessary expertise. Their involvement in criminal matters generally is rather limited, and it may be imposing an unfair burden to require them to consider these interprovincial applications.

(d) Leave the provisions as they are.

We basically favour leaving matters as they are, subject to one amendment to be discussed below. The various law enforcement agencies did not perceive this as a serious problem, and indicated that as a result of co-operation with other forces they had not encountered serious difficulties.

One problem was brought to our attention which we feel does warrant reform. This is as a result of the present wording of paragraphs 178.12(1)(*a*) and (*b*):

> (1) An application for an authorization shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction, or a judge as defined in section 482 and shall be signed by the Attorney General of the province in which the application is made or the Solicitor General of Canada or an agent specially designated in writing for the purposes of this section by
>
> > (*a*) the Solicitor General of Canada personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or
> >
> > (*b*) the Attorney General of a province personally, in respect of any other offence in that province, ...

The effect of these provisions is that a judge would seem to have no power to authorize an application where the offence is not being committed or was not committed in the province. Where an offence is committed in one province and the suspects were believed to be living in another province, it would seem that neither province could apply for an authorization. We expect that this is an oversight and that the legislation should be amended to permit authorities in one province to apply for an authorization, notwithstanding that the offence was committed in another. Moreover, such an amendment is consistent with our view that the authorization should primarily be person-oriented.

RECOMMENDATION

20. That subsection 178.12(1) be amended to provide that an authorization may be granted where the communications of the targeted person may be intercepted in one province, although the offence is alleged to have been committed in another province.

D. Minimization

While respect for privacy and restraint should be the important if not governing principles in the execution of such an intrusive investigative device as electronic surveillance, they generally receive minimal attention, once the order is granted. Thus, one of the most difficult challenges to any review of the present legislation is the question of minimization. Minimization is the procedure by which only those communications which are the proper subject of the investigation are intercepted and recorded. Unlike the United States federal legislation, Part IV.1 of the *Criminal Code* contains no explicit minimization requirement. An authorization will name certain persons, specify certain addresses and perhaps telephone numbers. It will as well contain a "basket clause" which permits the interception of unknown persons in contact with the named persons. The lines are ordinarily only monitored for two of three eight-hour shifts. Whether monitored or not, the recording devices operate automatically, recording all calls to and from the number. In addition, when the line is being monitored, a log is kept which sets out a brief summary of each call. Irrelevant calls are often noted as such.

Certain forms of surveillance are more closely monitored. However, even where the device is live monitored there is no policy requiring that irrelevant communications not be recorded.

The authorization in operation acts like a huge electronic vacuum cleaner, indiscriminately sucking in the relevant with the irrelevant without distinction. It has been represented to us by government people and the police that minimization requirements would destroy the effectiveness of wiretapping as an investigative tool. They point to the relative infrequency of use of wiretapping in the United States as a consequence of strict minimization requirements which make wiretapping a costly, inefficient investigative tool. We are not convinced that such is the case, in view of the American case-law to be dealt with *infra*, but it should be pointed out that wiretap legislation was intended to be the tool of last resort because of the serious implications to privacy and liberty. It is not self-evident that the legislation should be drafted to make wiretapping the preferred method of investigation.

Recent case-law has tended to encourage the erosion of what minimization safeguards there are in the legislation as it now exists. For example, in *R.* v. *Samson (No. 6)*,[102] the court considered that it was well within the bounds of a standard authorization to intercept the calls of tradesmen and other casual users of the targeted telephone, since their calls might include messages for the targeted individuals or other pieces of information which may assist in the investigation. So far as we are aware, except for the very rare case (for example, interception of a judge's or a lawyer's calls), the only minimization condition included in most authorizations is to require that visual surveillance accompany any interceptions at public telephones. This condition is not necessarily required by the present legislation, but is included "voluntarily" by the agents. It may be that judges would not otherwise authorize interceptions at public telephones if they were aware the authorization permitted it. (We should point out that a standard clause in most authorizations — the "resort to" clause — permits interceptions at all places, both stationary and mobile, to which the named persons may resort.)

It should be pointed out as well that this is one area where the Charter may have important implications. Additionally, Canada's obligations as a signatory to the United Nations *International Covenant on Civil and Political Rights* are of significance.[103] At the heart of these documents are respect for privacy and an obligation to protect against arbitrary and unreasonable infringements of that privacy. Questions could be raised as to whether it is unreasonable and arbitrary to sanction a system which permits the interception and recording of all telephone calls made to a certain telephone, irrespective of the user or the content of the conversation.

In our view, the key to an appropriate minimization requirement is recognition of the privacy interest. Interception should only be authorized where there is a basis for believing the targeted person is himself involved in criminal activity of the specified kind. We think that it is inconsistent with the Charter, our obligations as signatory to the *International Covenant on Civil and Political Rights* and the principles which should guide criminal procedure to permit widespread intrusions into the privacy of other persons on the tenuous basis that such interceptions may assist in an investigation. On the other hand, it is not necessarily unfair to permit interceptions and recording of all the calls of the named person, notwithstanding that some (even the majority) of these calls may not be "relevant." To require that only "relevant" calls be intercepted and

---

102. *R.* v. *Samson (No. 6)* (1982), 37 O.R. (2d) 48, 237 (Ont. Co. Ct.), reversed *supra*, note 58.

103. Canada is a signatory to the United Nations *International Covenant on Civil and Political Rights*, which entered into force on March 23, 1976, Article 17(1) of which states:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Both section 8 (unreasonable search and seizure) and section 7 (protection of life, liberty and security of the person) of the Charter recognize privacy as a fundamental attribute of a modern society. Of course, it remains to be seen whether section 7 in particular will be developed to reflect a broad right of privacy enforceable through the courts, as have the Fifth and Fourteenth Amendments in the United States through due process protection of "liberty." Thus, see L. Tribe, *American Constitutional Law* (New York: Foundation Press, 1978), especially Chapter 15: "Rights of Privacy and Personhood," and the discussion in the judgment of Parker A.C.J.H.C. in *R.* v. *Morgentaler, Smoling and Scott* (1984), 14 C.C.C. (3d) 258 (Ont. H.C.J.), pp. 299-314.

recorded may have important implications for the accused's right to make full answer and defence. It may be prejudicial and misleading to have available only the relevant, that is, incriminating part of a much longer conversation. One call taken out of context may have a very different interpretation when placed in the context of other calls by the accused. On the other hand, it places an almost impossible burden on the monitor to anticipate when the conversation will turn to the illegal activity.

To have truly effective minimization, the device would have to be live monitored at all times. While estimates vary, it is probably fair to say that this would at least triple the cost of any investigation. Accordingly, the gains to privacy have to be carefully assessed, and in the end we are not satisfied that the minimal gains to privacy which would accrue from requiring mandatory live monitoring in all cases are worth the immense increase in costs. We illustrate the minimal benefits by reference to the United States experience.

The leading case in the United States is *Scott* v. *United States*.[104] Under Title III[105] section 2518(5), the order must include a clause that the interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." While the order in *Scott* contained such a clause, agents intercepted *all* calls, only forty per cent of which related to the targeted offence (narcotic trafficking). The majority of the court concluded, however, that the minimization requirement was not infringed. The court adopted an objective reasonableness standard, rather than one which depended on an assessment of the police motives or good faith.[106]

If, as in *Scott*, the interception of *all* calls was lawful, even under a regime requiring live monitoring and minimization, then where is the significance or any gain to the privacy interest? Moreover, under any minimization procedure which could be suggested, privacy is still invaded, at least by the monitor. The only gain may be that the conversation is not tape-recorded so there is no permanent record. In our view, a mandatory statutory minimization requirement with mandatory live monitoring of the device is not justified. On the other hand, our consultants were all of the view that it would be helpful to have a list of minimization terms which the authorizing judge could include in the order in much the same way that subsection 663(2) of the *Criminal Code* contains a list of specific terms which a judge may include in a probation order. We believe that this represents a viable and practical solution to a very difficult problem.

A specific aspect of the minimization problem concerns solicitor-client and other privileged communications. As a result of an incident in which the telephone in the barristers' lounge in the Sault Ste. Marie courthouse was wiretapped, subsections (1.1) and (1.2) were added to section 178.13 of the *Criminal Code*. They provide as follows:

---

104. *Scott* v. *United States*, 436 U.S. 128 (1978).

105. Title III, *supra*, note 67, section 802, 82 *Stat.* 212.

106. See *supra*, note 104, pp. 139-41.

(1.1) No authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other such solicitor or a member of the solicitor's household has been or is about to become a party to an offence.

(1.2) Where an authorization is given in relation to the interception of private communications at a place described in subsection (1.1), the judge by whom the authorization is given shall include therein such terms and conditions as he considers advisable to protect privileged communications between solicitors and clients.

However, subsection 178.13(1.2) has recently been interpreted in *R.* v. *Chambers*[107] as not imposing any obligation on the judge to impose conditions to protect privileged communications. Anderson J.A., however, considered that "in most cases ... a protective clause should be inserted in the authorization to protect persons other than named targets."[108]

In our view, the intent of subsections (1.1) and (1.2) was to minimize interception of privileged communications, and that in such circumstances conditions must be mandatory.

A related problem concerns interception of privileged communications between a lawyer and client as the result of interceptions on the client's telephone. There is a certain analogy to search and seizure law in this respect. In *Descôteaux* v. *Mierzwinski*[109] the court held that solicitor-client privilege is not simply a rule of evidence, but rather has a much wider scope, and in fact has given rise to a substantive rule.

The rule formulated by Lamer J. proposes that the confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.[110]

While subsection 178.16(5) preserves the privilege with respect to admissibility of evidence, in our view the substantive rule, as formulated by Lamer J., has an implication at the interception stage which should be recognized in the legislation. It should be noted that in the recent case of *R.* v. *Heikel*,[111] Wachowich J. of the Alberta Court of Queen's Bench excluded all the wiretap evidence because of the repeated interception and recording of solicitor-client calls after the accused were first charged, notwithstanding that the Crown did not intend to adduce any of those conversations in evidence. His Lordship also objected to the repeated interception and recording of conversations between two accused who were husband and wife, although such conversations were

107. *R.* v. *Chambers* (1983), 9 C.C.C. (3d) 132 (B.C. C.A.).

108. *Id.*, p. 141.

109. *Descôteaux* v. *Mierzwinski* (1982), 70 C.C.C. (2d) 385, *per* Lamer J. (S.C.C.).

110. *Id.*, p. 400.

111. *R.* v. *Heikel*, Alta. Q.B., May 25, 1984, Wachowich J. (unreported).

also privileged. However, since the spousal communication privilege is strictly an evidentiary one and does not, it seems, give rise to a substantive rule,[112] we do not propose to make mandatory the minimization of such interceptions.

It will be observed that we have not specifically dealt with the consequences of failure to observe any conditions designed to implement minimization requirements imposed by the judge. This has proved an intractable problem in the United States (see, for example, *United States* v. *Dorfman*[113] and *United States* v. *Suquet*[114]). Since we recommend retention of the same admissibility rule as contained in present section 178.16, we see no reason to design special admissibility rules for minimization conditions. It will be for the trial judge to determine whether, in the particular case, the interception was made in accordance with the terms and conditions of the authorization, and thus lawfully made.

RECOMMENDATIONS

21. That an authorization may only be granted in relation to persons the interception of whose private communications will assist in the investigation of the offence by reason of their involvement in the offence.

22. That section 178.13 be amended to provide that the judge, in granting the application, may include any of the following terms and conditions:

(a) that the device be live monitored at all times that it is proposed to intercept or record private communications;

(b) that so far as is reasonably possible, only the conversations of targeted persons be intercepted and recorded;

(c) that where it is proposed to intercept communications at a telephone to which the public has a right of access, then any interceptions shall be on the basis of live monitoring and accompanied by visual surveillance;

(d) that reasonable steps be taken not to intercept private communications between spouses, physician and patient or persons in other confidential relationships;

(e) that reasonable steps be taken not to intercept private communications of targeted persons which by reason of a known pattern are unlikely to assist in the investigation of the offence;

(f) that interception cease after the object of the investigation has been obtained;

(g) that, where the interception of a telephone line will involve a party line, no interception occur except when the line is being monitored;

---

112. See: *Rumping* v. *Director of Public Prosecutions*, [1962] 3 All E.R. 256 (H.L.); *R.* v. *Kotapski* (1984), 13 C.C.C. (3d) 185 (Qué. C.A.).

113. *United States* v. *Dorfman*, 542 F.Supp. 345 (1982) (N.D. Ill.), appeal dismissed, 690 F.2d 1217.

114. *United States* v. *Suquet*, 547 F.Supp. 1034 (1982).

(h) such further terms and conditions as the judge considers advisable to minimize the acquiring and recording of private communications which would not assist in the investigation.

23. That the authorization shall include a term requiring that, where an interception is to occur at a place mentioned in subsection 178.13(1.1), reasonable steps shall be taken to ensure that privileged communications between solicitors and clients are neither intercepted nor recorded.

24. That where there are grounds to suspect that if an authorization is granted, privileged communications between the targeted person and his solicitor will be intercepted, that fact shall be disclosed in the application to obtain an authorization.

25. That in a case to which Recommendation 21 applies, the authorization shall include a term that, so far as reasonably possible, privileged communications between the targeted person and his counsel not be intercepted or recorded.

E. Basket Clauses

In *R.* v. *Welsh and Iannuzzi (No. 6)*,[115] the implications of failing to provide for the interception of unnamed individuals became apparent — the evidence of their conversations was inadmissible, since the interception had not been lawfully made. It has since been standard to include in an authorization a "basket clause" permitting the interception of communications of unknown persons. It should be pointed out that the basket clause is required only where the communication is between two persons neither of whom is named in the authorization. If at least one of the participants is named, then the interception is authorized and lawful, barring bad-faith concealment of the identity of one of the participants.[116]

The clauses that are included vary widely but are intended to meet the problem of getting before the courts the communications which were intercepted of persons who were not named in the authorization. The main point of litigation has become identifying the scope of the basket clause. It is often argued that the accused was known to the police at the time the authorization was obtained, and therefore interception of his calls was not authorized in a clause providing for "unknowns." It seems to us, however, that in terms of protecting privacy, this debate has few implications. This was also the view of the Supreme Court of the United States in *Donovan*.[117]

The issue from the privacy perspective is: To what extent should the law sanction and permit interceptions of persons who are not identified with the offence at the time

115. *Supra*, note 31.

116. *R.* v. *Gill* (1980), 56 C.C.C. (2d) 169 (B.C. C.A.).

117. *United States* v. *Donovan*, 429 U.S. 413 (1977).

the authorization is obtained? The problem also arises because of the threshold condition before which an individual is targeted, namely, any person "... the interception of whose private communications there are reasonable and probable grounds to believe may assist the investigation of the offence, ..."[118]

If electronic surveillance is considered a search or seizure within the meaning of section 8 of the *Canadian Charter of Rights and Freedoms*, then a statute which authorizes an unlimited basket clause may, to that extent, be unreasonable. In the United States, the consitutionality of Title III has been upheld in the lower courts, and by implication in the Supreme Court in *Donovan*. These cases focused on whether the legislation meets the requirements of the "warrant clause" of the Fourth Amendment.

In our view, this is not a satisfactory approach in the Canadian context. As Carr points out in *The Law of Electronic Surveillance*[119] the search warrant analogy is not very apt.

More to the point, in the Canadian context, is the absence of a warrant clause in section 8. While the Supreme Court of Canada has nevertheless held that there is a presumption in favour of a warrant as a prerequisite to a reasonable search,[120] it is not clear that there is a presumption in favour of any particular form of warrant.

There must be some provision, however, for unknown persons. These fall into two classes: (1) persons believed to be involved in the offence but unidentifiable; and (2) persons who are not only unidentified but whose existence may be wholly speculative at the time of the authorization. An example can be given to illustrate the two classes. Consider a narcotics investigation.

While it may be legitimate to permit the interception of conversations of any of these people, drafting legislation to permit such interceptions poses serious problems. A widely drafted basket clause becomes an invitation to indiscriminate interceptions and invasion of privacy. While some basket clauses are drafted so as to require a link between the offences, for example, "all persons, presently unknown resorting to certain premises for the purposes of committing one of the named offences," many are not, for example, "all persons found to be communicating with the named individuals at the specified premises."

While in our view the privacy interest could only be vindicated by a basket clause that would limit the interception to the conversations of persons of a class believed to be involved in the offence, this can create serious difficulties not only in drafting the clause but in its implementation. For example, one basket clause in common use in Ontario was as follows:

---

118. *Criminal Code*, s. 178.12(1)(e).

119. Carr, *supra*, note 67 (Supp., 1983), pp. 3-4.

120. *Supra*, note 37.

(3)(b) Authorization is also hereby given to intercept the private communications of persons whose identities are presently unknown, in accordance with the terms of this Authorization, provided that there are reasonable and probable grounds to believe that the interception of such private communications may assist the investigation of any of the offences stated in paragraph 1 above, whether or not any such person described in paragraph 3(a) above is party to such private communications.[121]

In other words, the clause repeated the test set out in paragraph 178.12(1)(*e*) of the *Criminal Code*, and as found by the Ontario Court of Appeal in *R.* v. *Paterson, Ackworth and Kovach*[122] was an unlawful delegation of the judge's function to the police. It was pointed out that it is the judge's function to determine the class of persons whose private communications may be intercepted under a basket clause. In our view, this is the correct approach. Furthermore, the judge must ensure that the basket clause is drafted so as to identify the appropriate group of persons, such as: permanent residents of the premises; habitual visitors believed to be involved in the offence; and so on. We believe that our recommendations are consistent with the interpretation in the *Paterson* case.

In our view, a basket clause is only legitimate if it permits the interception of the conversations of persons of a class known to be involved in the offence. Accordingly, a basket clause must be no wider than to permit interception of persons believed to be involved in the offence but unidentified at the time of the obtaining of the authorization.

Consistent with our view as to the proper scope of the interception, the threshold condition for targeting persons (known and identified) as presently contained in *Code* paragraph 178.12(1)(*e*) must be modified so as to replace the "assist in the investigation" requirement with a requirement of involvement in the offence as set out above in Recommendation 21.

One further concern about basket clauses is the use of a clause which permits installation of a device at other than named premises. When combined with a wide basket clause as to persons, one authorization can become very sweeping. While the need for the authorities to be able to respond quickly to changing locations is legitimate, this should be limited to the named persons to keep the scope of the authorization within reasonable bounds.

However, to avoid impediments to legitimate law enforcement objectives and yet improve judicial scrutiny, we believe there should be provision for the agent to return to the authorizing judge to obtain his approval of the wider use of the basket clause. Allied to this is a recommendation that the legislation direct the judge's attention to his right to insert a condition in the authorization requiring periodic reports as to the operation of the investigation. We do not envisage this as a normal condition but it

121. Excerpt of an authorization made by Judge McCart on June 10, 1982, and cited in *Paterson*, *infra*, note 122, p. 147.

122. *R.* v. *Paterson, Ackworth and Kovach* (1985), 18 C.C.C. (3d) 137.

may well be considered appropriate in certain sensitive investigations. Aside from these recommendations, we believe that *Code* sections 178.12 and 178.13 should remain as they are in respect of the granting of the original authorization.

RECOMMENDATIONS

26. That subject to Recommendation 27, the authorization shall contain a clause naming or otherwise identifying the persons the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

27. That, in addition, the authorization may contain a clause permitting the interception of a class of unidentified persons whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

28. That subject to Recommendation 29, the authorization shall limit the interceptions to specified premises.

29. That the authorization may contain a clause permitting interception of private communications at other than specified premises where the other place is resorted to by persons known and identified in the authorization. At such premises, only those communications to which the known and identified person is a party may be intercepted, unless the specially designated agent has applied in writing to the authorizing judge as soon as practicable for amendment of the authorization. The application for an amendment shall be supported by the affidavit of a peace officer setting out the reasons for interception at these premises, the names of the persons whose communications are likely to be intercepted and the reasons why interception at such premises is required. The judge may refuse to amend the order, or amend the order, which amendment is effective from the date when interception commenced at the additional premises, unless the judge is not satisfied that the application was made as soon as practicable, in which case the amendment may be made effective at such later date as the judge sees fit in the circumstances.

30. That the legislation contain a list of terms or conditions which *may* be included in the authorization, such as the following:

(a) that periodic reports be made to the authorizing judge as to the identities of persons whose communications are being intercepted pursuant to a basket clause;

(b) that periodic reports be made to the authorizing judge as to the places, not specifically named in the authorization, where interceptions are taking place.

F. Surreptitious Entry

By surreptitious entry, we mean the physical entry into private premises by law enforcement agents without the consent or knowledge of the occupier, for the purpose of installing a listening device. In the usual case, this means installation of a radio transmitter capable of transmitting oral communications to a location outside the premises where the communications can be recorded. While surreptitious entry may be used in some cases solely to install a device to assist in intercepting telephone communications, this is usually unnecessary and accordingly unusual. As a result of the decisions of the Supreme Court of Canada in *Lyons* v. *The Queen*[123] and *Wiretap Reference*[124] released on December 20, 1984, the present legal position may be summarized as follows:

(a) Unless the authorization contains limitations on or prohibition of surreptitious entry, an authorization by necessary implication authorizes any person acting under the authorization to enter any place at which private communications are to be intercepted to install or to service a permitted listening device, provided such entry is required to implement the authorization.

(b) The process of interception includes the installation of the device, and therefore an interception is only lawfully made within the meaning of paragraph 178.16(1)(*a*) if the installation was lawful.

(c) However, lawful means in accordance with Part IV.1, and therefore a surreptitious entry to install a device to implement an authorization being lawful, the interception would be lawfully made.

The McDonald Commission[125] favoured legislation with express power to authorize surreptitious entry in the national security field. This had two elements: first, the right to enter must be explicit and subject to certain limitations; and secondly, it must be permitted by a judge only in certain circumstances.

The Commission also made recommendations in the criminal investigation field, convinced that surreptitious entry was legitimate for the purposes of electronic surveillance[126] although not for search and seizure generally.[127] As indicated above, it was the McDonald Commission's view that surreptitious entry was not legal at present. Its Recommendation 265 is as follows:

WE RECOMMEND THAT section 178.13 of the Criminal Code be amended to permit peace officers executing authorizations under this section to take such steps as are reasonably

123. *Lyons* v. *The Queen*, [1984] 2 S.C.R. 631.

124. *Wiretap Reference*, [1984] 2 S.C.R. 697.

125. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Mr. Justice D.C. McDonald, Chairman, *Freedom and Security under the Law* (Second Report, 2 volumes) (Ottawa: Minister of Supply and Services Canada, 1981) (hereinafter cited as the McDonald Report).

126. *Id.*, vol. 2, pp. 1022-3.

127. *Id.*, vol. 1, p. 144; vol. 2, p. 1019.

necessary to enter premises or to remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing an interception device, providing the judge issuing the authorization sets out in the authorization

(a) the methods which may be used in executing it;

(b) that there be nothing done that shall cause significant damage to the premises that remains unrepaired;

(c) that there be no use of physical force or the threat of such force against any person.[128]

The Commission also noted that in the United States, despite a decision of the United States Supreme Court holding that surreptitious entry was lawful, constitutional legislation was under consideration to control surreptitious entry. The McDonald Commission referred to the evidence of the Assistant Attorney General, Criminal Division, before the Senate Judiciary Committee, wherein it was observed that:

> In the United States, despite the affirmation by the Supreme Court of the implied power of entry, the government has introduced a bill before the Congress which *expressly* provides for entry and for procedural safeguards to ensure that such methods will be used only when, as the Assistant Attorney General, Criminal Division, has said, "such methods have been found reasonable and necessary by an informed, impartial judicial officer."[129]

Moreover, notwithstanding the United States Supreme Court decision, it is the policy of the United States Justice Department to seek specific judicial authorization for a surreptitious entry.

The one dissenting voice in this area, as to the need for legislation, is the report prepared by the McLeod Committee[130] in response to the McDonald Report. The McLeod Committee was of the view that surreptitious entry was lawful and that legislation was not necessary to govern the area. While, as it turned out, the McLeod Commitee was right in concluding that surreptitious entry was not unlawful, for reasons set out below we are of the view that if surreptitious entry is to be permitted, it must be specifically dealt with by the legislation.

As indicated above, one of the cases that went to the Supreme Court originated as a reference directed to the Alberta Court of Appeal.[131] In the Court of Appeal, Chief Justice McGillivray and Justice Harrandence were of the view that surreptitious entry was lawful only if specifically authorized by the judge in the authorization. Both Justices saw the need for judicial control through appropriate conditions.[132]

---

128. *Id.*, vol. 2, p. 1023, Recommendation 265.

129. *Id.*, vol. 1, p. 175.

130. Federal/Provincial Committee of Criminal Justice Officials, *Report to Deputy Ministers of Justice, Deputy Attorneys General and Deputy Solicitors General by the Federal/Provincial Committee of Criminal Justice Officials with Respect to the McDonald Commission Report*, R.M. McLeod, Q.C., Chairman (Ottawa: Communications Division, Solicitor General of Canada, 1983) (hereinafter cited as the McLeod Committee Report).

131. *Reference re an Application for an Authorization* (1983), 10 C.C.C. (3d) 1 (Alta. C.A.).

132. See the comments of Chief Justice McGillivray, *id.*, pp. 14-5.

Mr. Justice Harrandence specified the conditions when surreptitious entry should be authorized:

> I am of opinion that if a superior court judge, on an application for an authorization made pursuant to Part IV.1 of the *Criminal Code*, determines that the public can *only* be served by the interception of private communications and that effective interception of those communications can *only* be obtained by placing a device on private property, then it is his duty to adapt the common law to meet modern conditions by authorizing a surreptitious entry or a suitable strategem to effect the installation of a device on that property.[133] [Emphasis in original]

The same concerns are echoed in the majority judgment in *Lyons* v. *The Queen* where Estey J., while holding the right of entry need not be explicit in the authorization, went on to recommend that it was a matter that should be considered by the authorizing judge.

> Having regard to the pattern of Part IV.1, the breadth of authority granted to the court, the importance of the subject-matter, and the vitality of the role of the court in the legislative plan as the guardian of the public interest, explicit response by the court to the application for authority to intercept in many cases will require the prescription of "terms and conditions advisable in the public interest" pursuant to para. (2)(*d*) of s. 178.13.[134]

Further, in *The Criminal Law in Canadian Society*[135] the position taken is that "the criminal law should provide and clearly define powers necessary to facilitate the conduct of criminal investigations." The Law Reform Commission has previously considered the problem of surreptitious entry.

In the Search and Seizure Working Paper, the Commission recommended that "[m]odifying search and seizure procedures to accommodate surreptitious police intrusions would result in serious sacrifices of the protective features of these procedures," and that "[a]bsent compelling evidence of the need for such sacrifices, the modifications should not be made in the context of criminal or crime-related investigations."[136]

It was pointed out that neither at common law nor by statute was surreptitious entry authorized for search and seizure. The Search and Seizure Working Paper essentially addressed the problem of intelligence probes and did not purport to deal with electronic surveillance. Nevertheless, the standard suggested for an exception may be appropriate, namely, Is there compelling evidence of the need for surreptitious entry in the area of electronic surveillance?

The figures that are available are ambiguous and unreliable in the attempt to determine whether surreptitious entry is necessary. Certainly it is probably fair to say that surreptitious entry is a relatively rare event. That is not surprising. Surreptitious entry

133. *Id.*, p. 28.

134. *Supra*, note 123, p. 671.

135. *Supra*, note 35, p. 61.

136. *Supra*, note 47, Recommendation 42, p. 260.

involves certain risks to the investigation. The officers may be caught installing the devices, or the devices may be discovered. Surreptitious entry may, as well, be difficult and involve expenditure of time and effort which can only be justified where there is a significant probability that evidence will be obtained which could not be obtained by the easier wiretap method. Nevertheless, surreptitious entry has been used in the electronic surveillance field and used effectively. Other devices such as parabolic microphones are not only less effective, but represent a greater likelihood of intrusion into the communications of innocent parties.

In Working Paper 30, two important problems were identified with surreptitious entry in the area of search and seizure. First, such entry was often justified in circumstances where grounds for a search warrant did not yet exist. This would not be a problem in the electronic surveillance area, since the entry would only be justified as a means of implementing the authorization. While some instances exist of police covertly entering premises to consider the feasibility of implanting microphones, this intelligence-gathering function cannot be justified independent of a judicial decision that grounds for an authorization to intercept private communications exist. As pointed out in Working Paper 30, "[t]o permit exploratory entries to ascertain whether such grounds exist is to render protection against unjustified intrusion extremely tenuous."[137]

A second problem identified in Working Paper 30 is that of reviewability and accountability. This is a serious problem in a regime of search and seizure which depends on announcement of entry, provision of documents to the occupier and allowing the occupant to witness the search. Modifications of these rules "would severely compromise the degree of protection associated with warrant procedure ...."[138] Again, however, there are not similar concerns in the electronic surveillance field. Even telephone wiretaps as presently authorized are done secretly and are quite different from the normal search and seizure. The policy decision to permit electronic surveillance is really a decision to permit the investigation to proceed in secrecy or covertly. The real issue in the electronic surveillance field is, What forms of secret intrusion should we permit and with what safeguards? This is not to discount the accountability problem but, as pointed out in Working Paper 30, it is a problem which pervades the electronic surveillance area.[139]

Since we favour a somewhat more open regime generally, some of these concerns will be addressed. Certainly, with respect to surreptitious entry, a special form of notification may be appropriate where no charges are laid and so reviewability and accountability through the trial process are not available. In its project on *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance*, the American Bar Association considered this problem and concluded:

> Inventory procedures can thus be worked out which would eliminate the most serious aspects of the objection to the surreptitious character of electronic surveillance: it needs, in short, to be surreptitious only initially. This objection, too, need not be controlling.[140]

137. *Id.*, p. 266.

138. *Id.*, p. 267.

139. *Id.*, p. 268.

140. *Supra*, note 50, p. 92.

But what of the privacy interest? How grave an intrusion is surreptitious entry? The entry itself is not meant to be discovered and therefore is ordinarily done with as little disturbance as possible, although this is not always the case.[141] The real intrusion is into the occupier's privacy subsequently, as a result of the capability of the device to pick up communications in the privacy of home or office, as indicated by Chief Justice McGillivray[142] in *Reference re an Application for an Authorization*, and Justice Estey in the *Lyons*[143] appeal.

Private thoughts are disclosed in home or office with no idea that they would even be disclosed in a telephone conversation. Since it represents such a serious intrusion into privacy, surreptitious entry to implant listening devices should only be permitted in very carefully circumscribed circumstances.

At the least, the right to make such entry should not be implied in every authorization, but must be the subject of prior judicial approval on the basis that, having regard to the seriousness of the particular offence and the likelihood of obtaining evidence, such an intrusion is justified. Further, conditions as suggested by the McDonald Commission in its proposed National Security Act would have to be imposed.

The recent Supreme Court decisions, however, did not deal with any implications which section 8 of the *Canadian Charter of Rights and Freedoms* might have for surreptitious entry.

It should also be pointed out that in *Dalia* v. *United States*,[144] the court found no infringement of the Fourth Amendment. In *Dalia*, the warrant had authorized interception of all oral communications "at the business office" of Dalia. The court concluded that by implication this was an authorization to make a covert entry which was not an unconstitutional infringement of the Fourth Amendment. The court was strongly of the view that Congress clearly understood that it was conferring power upon the courts to authorize covert entries ancillary to their responsibility to review and approve wiretap applications. By analogy to search warrants, there is no constitutional requirement that the electronic surveillance warrant set out the means by which it is to be executed.

We believe that the decision of the Supreme Court of Canada in *Hunter* v. *Southam Inc.*,[145] with its strong preference for prior judicial authorization to comply with section 8 of the Charter, strongly favours a statutory regime where the right to make surreptitious entry is explicit both in the legislation and in the authorization.[146]

---

141. There are apparently examples where a fire-alam was set off in order to empty the premises and provide access to the authorities to plant the device.

142. *Supra*, note 131, p. 12.

143. *Supra*, note 123.

144. *Dalia* v. *United States*, 441 U.S. 238 (1979).

145. *Supra*, note 37.

146. It is perhaps worth noting that Dickson C.J.C., who wrote the judgment of the court in *Southam*, *supra*, note 37, dissented in both *Lyons*, *supra*, note 123, and the *Wiretap Reference*, *supra*, note 124, being of the view that Part IV.1 of the *Code* did not permit surreptitious entry. Even the McLeod Committee Report conceded that the Charter could pose problems for covert entry.

A broad consensus emerged in our consultations that there was no basis upon which to limit the availability of surreptitious entry to certain serious offences, and that it was a matter that should be left for the individual judge to consider within certain guidelines. Nevertheless, in our view, surreptitious entry ought to be reserved for serious cases where there exists substantial likelihood that relevant evidence will be obtained.

We are firmly of the view that entry should only be effected in reliance on the authorization granted under Part IV.1 and should not be made by reliance on some other legal process such as a search warrant. As the Ontario Court of Appeal in *R. v. McCafferty* [147] pointed out, a search warrant must be strictly interpreted, and cannot be used to carry out a general search or used to plant a listening device.

Similarly, an entry under authority of an authorization is not authority to conduct a search of the premises although windfall information obtained during a covert entry could be the basis of an application for a search warrant to be executed in the normal manner.

A system of prior authorization depends, of course, on disclosure, to the authorizing judge, that the police will seek to use covert entry. We have been concerned as to the extent of disclosure required, and in particular, whether the means to be used to enter ought to be disclosed. It was forcefully represented to us that on the one hand there is a need for flexibility since the police may have to adapt their methods to changing conditions, and that on the other hand the judge lacking the necessary technical expertise would not likely be in a position to assess properly the viability or even desirability of one method over another. The concern, however, is over the use of inappropriate means to make the entry, such as sounding a false fire-alarm to clear the building. After considerable discussion, we have decided to opt for greater flexibility and not to require that the particular method to be used be disclosed in the application. If, in subsequent years, there should be abuse of the power, this position will of course have to be reconsidered, but at present we have no good reason to be concerned. We would, however, give the authorizing judge the power to deal specifically with certain means of entry if he considers it desirable.

RECOMMENDATIONS

31. That the authorizing judge be given power to authorize an entry onto private premises without the consent of the occupier, for the installation, removal or servicing of an electromagnetic, acoustic, mechanical or other device.

32. That the authorizing judge may only so authorize where the circumstances of the offence are serious and there is a high degree of likelihood that relevant evidence will be obtained.

147. *R. v. McCafferty* (1984), 13 W.C.B. 143 (Ont. C.A.).

33. That an application for an authorization which includes an authorization to make a surreptitious entry shall state the reasons why such entry is required and why other less intrusive means will not be sufficient.

34. That it be an offence to enter private premises without the consent of the occupier for the purpose of installing, servicing or removing an electromagnetic, acoustic, mechanical or other device without an order under Part IV.1 of the *Criminal Code*, and an offence to remove anything from the premises at the time of the entry.

35. That the peace officer making the entry should not be entitled to use force against any person for the purpose of effecting such entry or exit, except as necessary to protect himself or others.

36. That the authorizing judge may order that certain means be used/not used to effect the entry.

37. That following the investigation, the owner and occupier of the premises be notified of the entry and be given a copy of the order which authorized the entry.

38. That reasonable steps be taken to repair any damage to the premises or to compensate the owner for any significant damage left unrepaired.

39. That the use of a small amount of electricity to enable the device to function shall not constitute a criminal offence.

G. Renewals

The intrusiveness of electronic surveillance also arises from the length of time during which the intrusion takes place. For some investigations, the interception may extend over a period of many months. The *Criminal Law Amendment Act, 1977* extended the length of authorizations from thirty to sixty days.[148] While *Criminal Code* paragraph 178.13(2)(*e*) provides that the order may be valid for a period "not exceeding" sixty days, in fact, it is only on the very rare occasion that any order is for less than sixty days. By comparison, the United States legislation[149] provides for a maximum of thirty days and requires that the order contain a termination clause, that is, that the interception not continue for any period longer than is necessary to achieve the objective of the authorization. The average length of the American authorizations seems to vary from state to state and even county to county, but in most jurisdictions it approaches the

148. *Criminal Law Amendment Act, 1977*, S.C. 1976-77, c. 53, s. 9(3).

149. Title III, *supra*, note 67, s. 2518(4) and (5).

maximum permitted by statute. The efficacy of the termination clause is less than clear since, generally, the device is operated for the full term authorized.[150] (There are no statistics required by section 178.22 of the *Criminal Code* as to the duration of the interception.)

The Canadian legislation permits renewals or extensions for sixty-day periods.[151] The obvious purpose of a time-limit on the authorization is to place more temporal restraint on the interception to prevent the authorization from becoming an open-ended type of general warrant. Provision for a renewal or extension recognizes that some investigations may legitimately take longer than sixty days. However, consistent with the principle of restraint, there must be a demonstrated need for this further intrusion.

However, as the result of recent case-law, police rarely seek a renewal of an authorization. Rather, a new authorization will be sought even if only very minor changes are contemplated. In *R.* v. *Badovinac*,[152] the court held that a renewal could only extend the time of the original authorization but it could not "extend, modify, add to or otherwise deal with any feature of the authorization."[153] As pointed out in *R.* v. *Pleich*,[154] there are certain implications to legislation which favours obtaining a new authorization rather than a renewal. While on balance the requirements for an authorization set out in section 178.12 may be more onerous than the requirements for a renewal, it is those latter requirements which are really directed to the desirability of permitting the continuation of a wiretap investigation beyond the statutory limit. Subsection 178.13(3) provides for renewal of an authorization (1) upon an *ex parte* application, (2) accompanied by an affidavit of a peace officer or public officer deposing to the following matters, namely: the reason and period for which the renewal is required; full particulars of interceptions and information obtained; and the number of instances an application for renewal was made, withdrawn or refused — and (3) supported by such other information as the judge may require.[155]

While, as pointed out in *R.* v. *Pleich*,[156] the full and frank disclosure expected on an application under section 178.12 for a subsequent authorization would likely require the kind of information referred to in subsection 178.16(3), it is not statutory.

In our view, the legislation must be modified so that renewals are available where only minor changes are contemplated to the original authorization but the same investigation is being pursued. On the other hand, where the investigation has developed to the point where significant changes are needed, then a new authorization is appropriate.

---

150. *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications, 1983* (Washington, D.C.: Administrative Office of the United States Courts, 1983) (hereinafter cited as the Wiretap Report).

151. *Criminal Code*, s. 178.13(4).

152. *R.* v. *Badovinac* (1977), 34 C.C.C. (2d) 65 (Ont. C.A.).

153. *Id.*, p. 70.

154. *R.* v. *Pleich* (1980), 55 C.C.C. (2d) 13 (Ont. C.A.).

155. *Criminal Code*, s. 178.13(3).

156. *Supra*, note 154.

However, in the latter case there must be full disclosure of the extent of the prior investigation, so that the judge is in a position to consider the merits of the application properly.

We are also of the view that the longer the investigation, the greater intrusion, and hence the need for greater judicial scrutiny and responsibility upon the law enforcement officials. Accordingly, we propose that the normal term of a renewal be thirty days, unless grounds are shown for the longer period of up to sixty days. We believe that such an approach is more consistent with the principle of restraint. Of course, steps must be taken to ensure that the police have not applied for an authorization to take advantage of the longer period.

RECOMMENDATIONS

40. That where, to the knowledge of the designated agent or the deponent of the affidavit made in support of an authorization, an authorization has previously been granted in relation to the same or a related investigation, the application shall contain the information referred to in paragraph 178.13(3)(*b*) of the *Code*.

41. That a renewal of an authorization may include the names of persons previously provided for in the authorization but unnamed in the authorization.

42. That a renewal of an authorization may include additional places of interception of persons provided for in the original authorization.

43. That minor variations of the terms of the authorization may be included in a renewal, including the following:

(a) different or more accurate descriptions of persons or places;

(b) different or additional means of interception;

(c) different or additional offences clearly related to the offences in the original authorization and part of the same investigation.

44. That a renewal of an authorization may include terms not included in the original authorization, designed to minimize interceptions of communications which are not related to the offence.

45. That a renewal shall be for a period not exceeding thirty days, with the exception that where special cause is shown, a renewal may be for a period not exceeding sixty days. "Special cause" in this recommendation means circumstances making it probable that the investigation will not be completed within thirty days *and* it would be impracticable to obtain a further renewal within thirty days. Where the period of a renewal exceeds thirty days, the judge shall indicate on the face of the authorization the reasons therefor, with reference to the particular circumstances of the investigation.

46. That in any case referred to in Recommendation 45, the judge shall ensure that a renewal would not be available in the circumstances. In no case shall an authorization be granted where there is reason to suspect that it is intended to avoid the effect of Recommendation 45. Where the only reason that a renewal is unavailable is because the previous renewal or authorization has expired, then the subsequent authorization shall be for thirty days, unless special cause has been shown.

47. That the legislation provide for a list of terms and conditions which may be included in the renewal such as the following:

(a) that the interception shall terminate once the objective of the original authorization is achieved;

(b) that any applications for subsequent renewals or authorizations be made to the judge who granted the original authorization or renewal.

III. Reviewability and Secrecy

A. Introduction

While it is a fundamental feature of the Anglo-Canadian judicial system that judicial acts be open and subject to scrutiny by the public and higher courts, a feature which has now taken on constitutional dimensions,[157] another significant feature of Part IV.1 has been the lack of openness in the application process and judicial reticence to review subsquently the propriety of the application. Crown and police consultants have consistently represented to us that the internal controls in the application process, the necessity that the request for an authorization be reviewed by senior law enforcement officials and then by Crown counsel, ensure that only meritorious applications are brought forward. This, however, particularly in the case of such an intrusive means of investigation, misses the point, as Mr. Justice Jackson said in *Johnson* v. *United States*[158] in relation to the Fourth Amendment protection against unreasonable search and seizure. Such judgments should be made by a neutral and detached magistrate rather than an officer engaged in the actual investigation.[159]

It might well be asked, however, that the importance of involvement of the disinterested judicial official at the application stage having been accepted as a crucial element in securing the public from unreasonable invasion of privacy, What reason is

157. Paragraph 2(*b*) of the *Canadian Charter of Rights and Freedoms* as interpreted in *Re Southam Inc. and The Queen (No. 1)* (1983), 3 C.C.C. (3d) 515 (Ont. C.A.).

158. *Johnson* v. *United States*, 333 U.S. 10 (1948) (referred to in *supra*, note 46).

159. *Id.*, pp. 13-4.

there for further judicial scrutiny at the time it is sought to admit the evidence? The arguments in favour of openness after the execution of a search warrant have been made by Dickson J. in *Attorney-General of Nova Scotia* v. *MacIntyre*.[160] The point, it seems, is accountability to ensure against abuse of the very sweeping and intrusive powers placed in the hands of the police through search warrant and wiretap procedures. It would be ideal, perhaps, if every wiretap order could be subjected to subsequent judicial scrutiny to determine whether there has been abuse. This, however, is not practicable and is probably of little real benefit in gauging the likelihood of abuse. The fact is that essentially only in the context of the criminal trial process, where the liberty of the individual is at stake, are the resources available to scrutinize these procedures properly. It is only at that stage that the subject of the invasion has a sufficient interest and information to challenge the procedure, and the state a sufficient interest to defend properly the action taken by the authorities. Thus, the criminal trial process serves as the ultimate guardian of security of the privacy interest. The prospect that the actions will be subject to the intense scrutiny of the criminal trial protects the integrity of the entire system and shields the public generally from unreasonable invasion. There are, of course, costs associated with greater scrutiny: trials may be longer; police investigative techniques may be disclosed; "guilty" persons may be set free. The problem is to balance the privacy interests with these costs, recognizing that in view of these costs, the criminal trial process is an "inefficient" means of scrutinizing the functioning of the investigative process generally and especially in the area of electronic surveillance.

B. Review of the Authorization

The present provisions of the *Criminal Code* do not explicitly set out the grounds for review of the authorization. Review of the authorization is, of course, tied to the admissibility of evidence. While it may be that civil remedies could be sought for improper interceptions, the important questions arise in the context of the criminal trial process.

The threshold condition for admissibility of evidence in *Code* paragraph 178.16(1)(*a*) is that the interception was lawfully made. (There is also provision for admission by consent of one of the parties in paragraph 178.16(1)(*b*) but this involves different issues.) This paragraph roughly corresponds to section 2515 of Title III. Courts have construed this paragraph as permitting the admission of evidence where one of the parties to the communication consents to the interception so that it is not unlawful by reason of *Code* paragraph 178.11(2)(*a*).[161] The other ground for a lawful interception in paragraph 178.11(2)(*b*) is where the person "intercepts a private communication in accordance with an authorization ...." This requires that the Crown establish that the police were not only acting under an authorization, but that interception of the particular communication was authorized by the terms or conditions of the authorization. When the

160. *Supra*, note 96, pp. 144-7 (C.C.C.).

161. *Supra*, note 33.

legislation was first enacted, authorizations were not always as widely drafted as they are now, and the language used was not always as precise as it might have been. One of the first appellate decisions is a good example of an interception that was not made in accordance with the authorization. In *R.* v. *Welsh and Iannuzzi (No. 6)*,[162] it was held that an interception was not lawfully made when neither of the parties to the communication were named in the authorization, or otherwise provided for in the authorization. Another example is *R.* v. *Niles*.[163] These cases simply require the judge to look at the authorization and determine whether the particular interception fits within it.

These cases, however, shade into more difficult problems which raise issues as to the reviewability of the authorization. For example, where the authorization names certain persons as targets and also includes a basket clause for unknown persons, what of an accused who is unnamed but alleges he was known at the time the authorization was obtained? This can be looked at in two ways. On the one hand, the accused is not provided for on the face of the authorization: he is unnamed, yet not unknown so as to fall within the basket clause. This seems to have been the view of the Ontario Court of Appeal in *R.* v. *Crease (No. 2)*.[164] On the other hand, this also seems to be going behind the authorization. In order to determine whether the accused was meant to be included as an unknown for the purposes of the basket clause, the trial judge would need access to the secret packet so as to determine what material was before the authorizing judge. On its face, the authorization permits the interception of the accused as an unknown person. This approach essentially equates unknown with unnamed, and is not entirely persuasive. It was, however, accepted by the majority of the British Columbia Court of Appeal in *R.* v. *Lloyd and Lloyd*.[165] It should be noted that, in the *Lloyd* case, there was no allegation of fraud or wilful nondisclosure.

The known/unknown problem can shade into a true question of going behind the authorization. For example, where the allegation of the accused is not merely that he was "known" at the time the authorization was obtained, but that his identity was not revealed to the authorizing judge, deliberately, because had the judge known of the police intention to intercept his communications (either under the basket clause or as party to a communication with a named person), the authorization would not have been granted. In *R.* v. *Gill*,[166] the evidence obtained was held to be inadmissible after the judge found that the police had concealed their intention to intercept the communication of the unnamed person and that they intended to intercept the communication between the accused (who was named) and the unnamed person in the jail after the arrest of the accused. The court of appeal held that none of the conversations between the two were admissible in view of the defects in the obtaining of the authorization. It is interesting that the court's approach was not to determine whether the authorization was

162. *Supra*, note 31, pp. 13-4 (O.R.), p. 375 (C.C.C.).

163. *R.* v. *Niles* (1978), 40 C.C.C. (2d) 512 (Ont. C.A.).

164. *R.* v. *Crease (No. 2)* (1980), 53 C.C.C. (2d) 378 (Ont. C.A.).

165. *R.* v. *Lloyd and Lloyd* (1980), 53 C.C.C. (2d) 121, 16 C.R. (3d) 221, (B.C. C.A.), reversed in part on other grounds (1982), 64 C.C.C. (2d) 169, 131 D.L.R. (3d) 112, 39 N.R. 474 (S.C.C.).

166. *Supra*, note 116, p. 176.

rendered void, voidable or unenforceable, but merely to treat the question solely as one of admissibility. The court, in ruling the communication inadmissible, relied on the wording of former paragraph 178.16(2)(*b*) which, like the present subsection 178.16(3), refers in an oblique way to substantive defects (as opposed to defects in form) in the application for the authorization.

The other issue which clearly presents a reviewability problem is raised in *Wilson* v. *The Queen*.[167] In that case, the trial judge found a substantive defect in the application based on evidence at trial that led him to conclude that none of the pre-conditions in paragraph 178.13(1)(*b*) had been met. He arrived at his conclusion solely on the basis of *viva voce* evidence without examining the sealed packet. All members of the court considered that he was in fact going behind (reviewing) the authorization and that the procedure was improper. The court divided, however, on the proper procedure. The majority *per* McIntyre J. essentially disagreed with the *Gill* approach and held that subsection 178.16(3) gives no jurisdiction to exclude evidence for substantive defects where the interception was made in accordance with an authorization, valid on its face. By implication, however (and by analogy to civil cases where *ex parte* orders are granted), where the authorization was improperly obtained it can be set aside by the authorizing judge. Presumably then, any interception which had been made pursuant to the now invalid authorization would be retroactively rendered unlawful and the communication inadmissible.

In his minority judgment, Dickson J. would permit collateral attacks to the authorization by the trial judge, but considered that the trial judge erred in holding that he did not need to consider the contents of the sealed packet to determine whether there was a defect in the application for the authorization.

Under either scheme, the procedure contemplated is a cumbersome one. If the attack on the authorization must be made before the authorizing judge, this may entail substantial delay and interruption of ongoing trials. Even under the procedure suggested by Justice Dickson, there will be delay if, as in *Wilson*, the trial is before a provincial court judge who has no power to open the sealed packet under section 178.14 of the *Code*.

Other problems relate to the grounds for review or setting aside the order, the pre-conditions, if any, before which the sealed packet can be opened, and if there is a burden on the accused to establish a defect in the application, how to discharge the burden without access to the sealed packet.

McIntyre J., in referring to civil cases, appears to consider "fraud or the discovery of new evidence" as grounds for setting aside the *ex parte* order. In referring to the possibility of another judge of the same court hearing the review due to the exigencies of court administration, he stated: "... the reviewing judge must not substitute his discretion for that of the authorizing judge. Only if the facts upon which the authorization was granted are found to be different from the facts proved on the *ex parte*

167. *Wilson* v. *The Queen* (1983), 9 C.C.C. (3d) 97 (S.C.C.).

review should the authorization be disturbed."[168] One might well ask where the evidence of different facts is to come from. The majority judgment raises the spectre of lengthy preliminary hearings in an effort to discover new facts as a foundation for the review.

In his concurring judgment, Mr. Justice Dickson did not enumerate the grounds for review of validity, but noted the cases which have refused access to the sealed packet except where there is a *prima facie* case of fraud or nondisclosure, to which he added misleading disclosure. He appears to contemplate that the grounds for review could emerge during cross-examination at trial of the deponent of the affidavit.[169]

Again however, the spectre of undue waste of time is raised. Defence counsel under the scheme are required to conduct a fishing expedition. They must grope around in the dark hoping to turn up something which gets them into the sealed packet, without knowing what that something even looks like.

The final area of review is noted by Dickson J. This is facial invalidity. For example, the authorization fails to specify the period for which it is in force, or the date when it was granted. It is to these perhaps technical defects which the curative provision in subsection 178.16(3) appears directed.

The problems presented by review in particular, going behind the authorization, are serious and fundamental from a position both of policy and procedure. In our view, these problems can only be overcome by a clear statement as to the grounds and procedure for review and access to material.

American courts have had a somewhat longer and different experience under Title III and a survey of that experience may prove helpful. Sections 2518(9) and (1)(a) of Title III contemplate much freer access to material than is the case under Part IV.1. Section 2518(10)(a) also sets out the grounds for "suppression" of the evidence:

> Any aggrieved person in any trial, hearing or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that —
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[170]

The question of review really revolves around ground (i). In *United States* v. *Giordano*,[171] the court considered the meaning of "unlawfully intercepted" in (i) and concluded that the words are not limited to constitutional amendments, as:

168. *Id.*, p. 97.

169. *Id.*, p. 112.

170. Title III, *supra*, note 67, s. 2518(10)(a).

171. *United States* v. *Giordano*, 416 U.S. 505 (1974).

> Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations calling for the employment of this extraordinary investigative device.[172]

Subsequent litigation has turned on what requirements were designed to "directly and substantially implement" the congressional intent, or put another way, which provisions "play a central role in the statutory scheme."[173]

C. Fishman, in his text, *Wiretapping and Eavesdropping*, has compiled a list on "central" and "non-central" provisions as follows:[174]

Central

1. AUTHORIZING OFFICIAL: 18 USCS s. 2516(1) (federal) and (2) (state).
2. DESIGNATED OFFENSES: 18 USCS s. 2516(1) (federal) and (2) (state).
3. PROBABLE CAUSE: 18 USCS ss. 2518(1)(b)(i-iii) and 2518(3)(a,b,d).
4. NORMAL INVESTIGATIVE PROCEDURES: 18 USCS s. 2518(1)(c) and (3)(c).
5. THIRTY-DAY MAXIMUM PERIOD: 18 USCS s. 2518(5).
6. TERMINATE UPON ATTAINMENT OF AUTHORIZED OBJECTIVE: 18 USCS s. 2518(4)(e) and (5).
7. PRIOR APPLICATIONS: 18 USCS s. 2518 (1)(e).

Non-Central

1. IDENTIFYING THE AUTHORIZATION OFFICIAL: 18 USCS s. 2518(1)(a) and (4)(d).
2. IDENTIFYING THE TARGETS IN THE APPLICATION: 18 USCS s. 2518(1)(b)(iv).
3. IDENTIFYING THE TARGETS IN THE WARRANT: 18 USCS s. 2518(4)(a).
4. INVENTORY AND NOTICE: 18 USCS s. 2518(8)(d).

Numbers (3) and (4) of the "central" provisions and numbers (2) and (3) of the "non-central" provisions, require most careful scrutiny, since they are the grounds which could arise or have arisen under the Canadian legislation. In this area, the leading case is *United States* v. *Donovan*,[175] which held that:

> [A] wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in the criminal activity under investigation and expects to intercept the individual's conversations over the targeted telephone.[176]

This was in accord with the earlier decision in *United States* v. *Kahn*.[177]

---

172. *Id.*, p. 527.
173. *Id.*, p. 528.
174. C.S. Fishman, *Wiretapping and Eavesdropping* (Rochester, N.Y.: The Lawyers Cooperative Publishing Co., 1978), pp. 372-6.
175. *Supra*, note 117.
176. *Id.*, p. 428.
177. *United States* v. *Kahn*, 415 U.S. 143 (1974), p. 155. The court then rejected a requirement that the order identify all persons whom the government could have discovered by diligent investigation.

It was held that section 2518(10)(a)(i) did not require suppression of Donovan's conversations. The court took a somewhat practical approach, asking the question whether it would have made a difference to the authorizing judge.[178]

The reasoning in *Donovan* demonstrates why, if the probable cause for the normal investigative procedures requirements is not met, the evidence would be suppressed. Clearly, if the judge knew that, for example *per* section 2518(3)(c), normal investigative procedures have been tried and have succeeded, he would not have been empowered to grant the warrant. Moreover, the section 2518(3) requirements, like the *Code* subsection 178.13(1) requirements, underpin the congressional/parliamentary intent to limit the resort to this extraordinary and highly intrusive method of investigation.

Certainly, the *Donovan* approach is sufficient to vindicate the restraint principle. The question remains, Is it sufficient to vindicate the privacy interest? We think that it probably is. On the other hand, the investigation into known/unknown does not really advance the privacy interests, except in the case where it could be said that the judge would not or could not have granted the authorization, had he known the true scope of the intended targets (*Gill*[179]), or had he known the possibility of indiscriminate interception of "unknown" targets. We think this latter problem is one of minimization and can often involve very fine distinctions. Where it is apparent that the authorization would be granted for the primary targets, it hardly advances the protection of privacy to require the police to *include*, as targeted individuals, persons who may be only marginally involved because failure to do so might invalidate the authorization. This will simply have the effect of enlarging the scope of the wiretap investigation rather than restraining it. Where an apparent primary target is not identified, then an inference of oblique motive would arise and would be properly dealt with under the rubric of *Gill*-type reasoning.

As noted above, section 2518(10)(a) of Title III gives as a third ground for suppression that the interception was not made in conformity with the order of authorization. This is similar to the way *Code* paragraph 178.16(1)(*a*) has been interpreted and poses no new problems.

Since *Wilson*, there have been a few decisions by authorizing judges who have been asked to set aside their orders. To date, no firm principles have emerged as to when the judge will be prepared to: (1) open the packet; or (2) set aside the order. In *R.* v. *Delhaye*,[180] O'Leary J. opened the packet and set aside the order, it seems, simply because he found that the affidavit had not disclosed the identities of two of the parties, the interception of whose conversations there were reasonable and probable grounds to believe would assist the investigation. That seems a drastic result. There is nothing in the judgment to indicate that this omission was done in bad faith (as *per Gill*), nor any reasoning as to why the entire order was set aside. Significantly, O'Leary J. did not ask himself the question whether he would have granted the order knowing the true

178. *Supra*, note 117, p. 435.

179. *Supra*, note 116.

180. *R.* v. *Delhaye*, Ont. H.C.J., March 7, 1984, O'Leary J. (unreported).

state of affairs: (a) as it was; (b) including the two individuals; (c) specifically excluding the two individuals as targets; (d) not at all. This may well be because of the lack of any guidance in *Wilson*[181] as to when the authorization may be set aside, except for the rather unhelpful comment by McIntyre J., referred to earlier, based on cases dealing with setting aside *ex parte* orders in civil cases.

In another post-*Wilson* case, *R.* v. *Con and Fung*,[182] another practical problem with the *Wilson* procedure was pointed out. In that case, the authorizing judge, Huddart Co.Ct.J., was asked to make findings as to the state of knowledge of the police about the identity of one of the conspirators and the availability of other normal investigatory techniques, based upon testimony adduced in other proceedings. Some of the evidence was conflicting and required findings of credibility. His Honour observed that he was "at a considerable disadvantage in assessing the weight to give to [the investigating officer's] evidence." Judge Huddart was also confronted with the problem as to when he was justified in opening the packet on the basis of an allegation that at least one of the criteria in paragraph 178.13(1)(*b*) had not been met. He concluded that this was not sufficient, as there must be *prima facie* evidence on all three criteria before the sealed packet is opened, or alternatively, there must be evidence of deliberate deception with regard to one of the criteria. The fact that one criterion has not been met is not sufficient.[183]

C. Secrecy

Closely allied to the problem of reviewability is that of access to materials. *Code* section 178.14 contains quite exceptional provisions for keeping the material filed on the application secret, by placing it in a sealed packet to be kept in the custody of the court, and to be opened only for the purpose of dealing with an application for renewal or pursuant to an order of a judge referred to in the section.[184]

While subparagraph 178.14(1)(*a*)(ii) gives a section 482 judge power to open the packet, that jurisdiction has been narrowly construed. A representative case is *Re Stewart and The Queen*[185] where Mr. Justice Krever held that the power to open the sealed packet "is a power to be reserved for the exceptional case"[186] and that the "circumstances must be rare"[187] when the jurisdiction would be exercised.

181. *Supra*, note 167.
182. *R.* v. *Con and Fung* (1984), 11 C.C.C. (3d) 396 (B.C. Co.Ct.).
183. *Id.*, p. 404.
184. *Criminal Code*, s. 178.14(1).
185. *Re Stewart and The Queen* (1976), 30 C.C.C. (2d) 391 (Ont. H.C.J.).
186. *Id.*, p. 401.
187. *Id.*, p. 402.

While Krever J. did not articulate the grounds which *would* justify an order under subparagraph 178.14(1)(*a*)(ii), other cases such as *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*,[188] have limited the circumstances to those of fraud and similar misconduct by the authorities.

Section 178.14 also stands in the way of a person who has been the object of an interception and so notified under section 178.23, but not charged. That person is virtually cut off in any attempt to challenge the legality of the authorized interception by the secrecy provisions.[189]

The grounds for opening the packet paralleled the grounds for reviewing the authorization in the pre-*Wilson* cases. As Zuber J.A. indicated in *R.* v. *Welsh and Iannuzzi (No. 6)*,[190] such grounds "would include cases in which the authorization was defective on its face, or was vitiated by reason of having been obtained by a fraud."[191]

An authorization can only be set aside on the basis of fraud or wilful nondisclosure. To ascertain whether there has been fraud or wilful nondisclosure, the defence needs access to the sealed packet, but to gain access it must show fraud or wilful nondisclosure. The way that some counsel have attempted to break the circle is to cross-examine the police officer who made the affidavit. The logical inconsistency of this tactic has not escaped the courts. Thus, in *R.* v. *Haslam*,[192] it was held that the officer could not be cross-examined on the contents of the affidavit in the absence of an order under *Code* section 178.14. Leaving for a moment the question of review, the secrecy provisions raise other problems:

(a) limited empirical data as to the scope of basket clauses;

(b) virtually no data as to whether the statutory prerequisites in fact existed — for example, that other investigative measures had been tried and had failed;

(c) virtually no data as to whether basket clauses are in fact resorted to for the interceptions;

(d) virtually no data as to whether monitoring of the devices takes place;

(e) virtually no means of determining the seriousness of the case in which the interceptions take place.

These are primarily problems of openness and accountability and the Law Reform Commission is on record as favouring to the greatest extent possible openness and reviewability of the conduct of law enforcement agencies. An argument favouring

188. *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)* (1978), 40 C.C.C. (2d) 212 (Alta. S.C.), p. 219.

189. *Re Zaduk and The Queen* (1979), 46 C.C.C. (2d) 327 (Ont. C.A.). This particular problem is discussed *infra* under the heading "VI. B. Notice under Section 178.23."

190. *Supra*, note 31.

191. *Id.*, pp. 371-2 (C.C.C.).

192. *R.* v. *Haslam* (1977), 36 C.C.C. (2d) 250 (Nfld. Dist. Ct.).

' openness' in respect of judicial acts was forcefully put by Dickson J. in *Attorney-General of Nova Scotia* v. *MacIntyre*[193] in relation to search warrants, and can also be applied to other areas of police powers.

Mr. Justice Dickson went on to indicate that the concern for accountability is not diminished by the fact that the search warrants might be issued by a justice *in camera*, but, rather "this fact increases the policy argument in favour of accessibility." He indicated that "what should be sought is maximum accountability and accessibility but not to the extent of harming the innocent or of impairing the efficiency of the search warrant as a weapon in society's never-ending fight against crime," and concluded that "curtailment of public accessibility can only be justified where there is present the need to protect social values of superordinate importance. One of these is the protection of the innocent."[194]

The question then is whether, in the field of electronic surveillance, secrecy is required to "protect social values of superordinate importance." Two values have been identified by the police and government representatives: protection of informers, and protection of police investigative techniques. It has also been forcefully put to us that the present system of confidentiality encourages greater candour in the material before the authorizing judge, and that if there were a more open regime, police and agents would be less likely to place the entire picture before the judge for his consideration. This last issue is an important one where the *only* method of accountability is the prior judicial approval. It is less important if other post-interception review procedures exist. This is not to discount the importance of this consideration, but it may be somewhat exaggerated, as evidenced by the experience of the McDonald Commission.[195]

What then are the societal values on the other side of the issue?

1. *Restraint*: The very high proportion of authorizations granted as compared to those of the United States leads to the conclusion that authorizations are applied for in circumstances where the crimes under investigation are not serious and other methods of investigation would be more appropriate — that is, there is an unjustified pervasiveness of a very intrusive device.

2. *Accountability*: There is essentially no check on the truth of the material filed in support of the application after the granting of the authorization.

3. *Review*: Opportunities by the accused to test the lawfulness of the application are essentially frustrated.

4. Individuals who have not been charged but have been targeted are prevented from testing the lawfulness of the application and the interception in civil courts.

193. *Supra*, note 96.

194. *Id.*, pp. 144-7 (C.C.C.).

195. Supra, note 125, vol. 2, pp. 1021-2.

D. Conclusion

As indicated above, the problems of review and secrecy are closely related and any solution to the reviewability issues depends on the degree of access to materials. It was therefore proposed that we adopt a procedure whereby the accused would be given complete access to the material used on the application, as is done in the United States. The viability of this procedure was presented to our consultants and there was almost complete agreement that, subject to a method to protect the identity of informers and persons assisting the police, there was no reason not to give the defence complete disclosure. The consultants were frank in stating that they saw no serious problems in terms of disclosure of police investigative techniques. They did not envisage any significant chilling effect on the quality of the material which would be presented on the application. While concerns were expressed that the names of suspects who were never charged would be disclosed, on balance it was felt that the gains in terms of accountability, and even trial efficiency, more than outweigh these problems. As it was pointed out, even under the present system the identity of persons named in the authorization is disclosed during the trial even if some of those persons are not charged. One further concern expressed was the problem that disclosure might interfere with other ongoing but related investigations. However, the consensus was that this would hardly ever be a problem and that, when the issue arose, the Crown would simply have to make the decision as to whether and when to lay charges. This is a problem which is not unique to electronic surveillance, and a special rule could not be justified. The problem of police informers is different. They have always enjoyed special status and protection which has been reaffirmed in very explicit and almost absolute terms by the Supreme Court of Canada.[196] As well, there is a real potential of personal danger to the informant should his identity be disclosed. A solution adopted in the United States is to attempt to draft the material used in the application so as to shield the identity of the informer. We favour a much more direct approach by providing for an *ex parte* application to a judge to seal or delete portions of the affidavit.

Finally, concerns were raised about disclosing the identity of persons who, while not true informers, agree to assist the police on a promise of confidentiality. An example was given of a home owner who may permit the police to use his house as a surveillance point. It was suggested that in certain cases it may be necessary to disclose that person's identity in the affidavit to obtain the authorization, but no real interest was served by disclosing the identity publicly. Since these cases are roughly analogous to cases of police informers, we feel that they too could properly be brought within the procedure for sealing portions of the material. The question then is, When and how should review of the authorization take place, and what are the consequences of that review? The *Wilson*[197] application seems totally unsatisfactory. It can result in substantial delay and disruption of the orderly trial process. Since reviewability of the authorization is tied

196. See, for example: *Bisaillon* v. *Keable* (1983), 7 C.C.C. (3d) 385, 2 D.L.R. (4th) 193 (S.C.C.); *The Solicitor General of Canada* v. *The Royal Commission of Inquiry into Confidentiality of Health Records in Ontario*, [1981] 2 S.C.R. 494, 62 C.C.C. (2d) 193.

197. *Supra*, note 167.

to admissibility of evidence, it should be handled at the trial or preliminary inquiry as the case may be. Broadly speaking, there are two categories which could be grounds for review of the application process: mistake and fraud.

By "mistake" we mean that the judge erred in granting the authorization because on its face there were not sufficient grounds set out in the application upon which a judge, acting judicially, could have made the order. By "fraud" we mean that while the application and affidavit are valid on their face, evidence is available to demonstrate that the facts are not as represented in the affidavit, or there has been wilful omission of pertinent facts. Theoretically, either basis could be grounds for holding that there has been such a defect in the application procedure as to require a sanction. The issue is, however, whether the appropriate sanction is inadmissibility of evidence in both cases. For reasons developed *infra*, under the heading "V. Remedies," we have determined that only the "fraud" category is a sufficient basis for exclusion of evidence. It follows therefore that reviewability of the application process must be limited to those grounds. Other civil remedies for the individual may be available or have to be fashioned where an authorization is mistakenly granted for insufficient reason. Aside from that, we would like to see a review after several years by a panel of experts to determine whether there has been compliance with the provisions of *Code* sections 178.12 and 178.13. With the more liberal disclosure provisions, such a review would now be possible.

If we accept that evidence will be inadmissible where there is a substantive defect in the application as defined *infra* (that is, broadly speaking for fraud), the issues then become merely procedural.

(1) Issue One: Where Is the Question Resolved?

One of the consistent criticisms of the wiretap legislation has been the length of the *voir dire* proceedings to resolve questions of admissibility. Thus, if at all possible, this ground for review should not add appreciably to the length of the proceedings; multiplicity of proceedings should be avoided. On the other hand, we think it will be a rare case where an evidentiary hearing will be required to resolve these issues in view of the definition of substantive defect in the application. A determination at the preliminary inquiry may seem a waste of judicial time. The finding does not bind either party in any subsequent proceedings.[198] On the other hand, an accused has the right to make full answer and defence at the preliminary inquiry and traditionally, the same evidentiary rules have applied at the preliminary inquiry as at the trial.[199] An accused could justifiably complain that he should not be put to the expense and embarrassment of a trial if the only evidence against him is inadmissible. These are all very cogent arguments, and in the end a policy choice must be made. Because we do not believe

198. *R.* v. *Duhamel* (1984), 57 N.R. 162 (S.C.C.).

199. *R.* v. *Pickett* (1975), 28 C.C.C. (2d) 297 (Ont. C.A.); *Re Stillo and The Queen* (1981), 60 C.C.C. (2d) 243 (Ont. C.A.).

that the hearing required will unduly protract the proceedings, we have opted for permitting a challenge to the application procedure to be made at the preliminary inquiry and at the trial.

(2) Issue Two: How Is the Question Resolved?

By reason of the proposed amendment to section 178.14, the accused will have access to almost all of the material used on the application. He can then review that material with his legal advisers and, after conducting whatever investigation he feels appropriate, consider whether there is any basis for challenging the material on grounds of fraud or recklessness on the part of the authorities (the test for inadmissibility as set out in Recommendation 63). In our view, there is an onus on the accused at least to make the issue of a substantive defect a live one before he is entitled to an evidentiary hearing at which the police officers would be compellable witnesses. We would contemplate that the foundation for an evidentiary hearing could be laid by affidavit evidence, which would not, however, be admissible against the accused on the trial proper.[200] The judge would be required to determine whether there is a sufficient basis to conduct a further evidentiary hearing. Obviously, if the affidavit material merely reveals inaccuracies of trifling significance, which could in no way raise a real question as to the integrity of the application procedure, then there would be no basis for ordering a further hearing.

However, where the material raises a real question as to whether there has been a substantive defect in the application, then there must be a full inquiry by the judge. In view of the nature of the grounds of admissibility, we believe that the burden of proof is properly on the Crown to demonstrate the integrity of the application process. It will have complete access to the files and the personnel involved, and be in the best position to lead evidence to resolve the issues properly.[201]

RECOMMENDATIONS

48. That section 178.14 of the *Criminal Code* be amended to include the following:

(a) in addition to the exceptions provided for in present paragraph (1)(*a*), to allow access to the material in the sealed packet for the purpose of dealing with an application for an authorization in related investigations;

(b) to permit the specially designated agent to retain a true copy of all the documents relating to an application made pursuant to section 178.12 or subsection 178.13(3).

200. A similar rule seems to apply with respect to an accused's *voir dire* testimony. See *Erven* v. *The Queen* (1978), 44 C.C.C. (2d) 76 (S.C.C.).

201. The procedure suggested is similar to the comparable American procedure. See Carr, *supra*, note 67, pp. 349-50; *Franks* v. *Delaware*, 438 U.S. 154 (1978); *United States* v. *Licavoli*, 604 F.2d 613 (1979) (9th Cir.).

49. That the prosecutor, when giving notice under subsection 178.16(4), shall include: a copy of the authorization and renewals under which the interceptions were made; and, subject to the order of a court, a copy of all the documents relating to an application for the authorization or renewal.

50. That prior to giving notice pursuant to subsection 178.16(4), the specially designated agent may apply to a judge as defined in section 482 of the *Criminal Code ex parte* and *in camera* for an order that certain portions of the material not be disclosed on the basis that disclosure could tend to reveal the identity of an informer or of any other person who has assisted with the investigation and in the latter case it is shown that it would not be contrary to the public interest that the identity of such persons be withheld. The application should be in writing and supported by the affidavit of a peace officer.

51. That the person against whom evidence is sought to be admitted pursuant to paragraph 178.16(1)(*a*) of the *Criminal Code* by reason of an interception made pursuant to an authorization or renewal, may apply at the preliminary inquiry or the trial to exclude that evidence and derivative evidence on the basis of a substantive defect in the application for the authorization or renewal. The following procedure would apply:

(a) The application should be in writing and supported by affidavit evidence (or *viva voce* evidence with leave of the judge).

(b) Only if the application and the evidence in support when considered together with the material disclosed under Recommendation 49 raises a real question as to whether there is a substantive defect in the application as defined in Recommendation 62 which could lead to the exclusion of evidence, shall the judge hold an inquiry as to the validity of the application for the authorization or renewal.

(c) Should the judge direct an inquiry, the burden of proof is on the Crown to satisfy the court that there was no substantive defect in the application as defined in Recommendation 62.

(d) The affidavit and testimony of the accused is not admissible at the instance of the Crown at the preliminary hearing or trial.

IV. Emergency Authorization: Section 178.15

A problem under the emergency authorization procedure which was drawn to our attention was that of the kidnap victim. It would seem that there is a desire among some law enforcement agencies to be in a position to conduct electronic surveillance immediately should they learn the whereabouts of the kidnap victim, without even having to resort to the emergency procedure under section 178.15. It was suggested that such interceptions could be rendered lawful by deeming the victim of the offence to have consented to any interceptions. On the whole, it is not clear to us that this

would advance the situation, since it is unlikely that the victim would be party to many conversations. Interception of communications to the person who is the victim of extortion would already be lawful, if done with the actual consent of that person. In the one reported case which makes any reference to this issue, *R.* v. *Gamble and Nichols*,[202] it would seem that the police did have time to obtain an authorization (which, however, was held to be defective).[203] In our view, all that is required is a slight modification of section 178.15 to provide some lead time to the police in these very dangerous situations.

A further problem with section 178.15 is the absence of a record of what has taken place. While subsection 178.15(2) requires that the authorization be in writing, there is no requirement that the application be in writing. In the result, it is virtually impossible to review the application subsequently. In our view, particularly in light of our recommendations concerning disclosure, it is desirable that there be some record of the application; for this purpose, the telewarrant procedure, as proposed in section 70 of Bill C-18 which would add section 443.1 to the *Criminal Code*, would appear to be the simplest and most effective mechanism for recording the facts relied upon by the judge in granting the authorization. The facts which would be required to be set out would be: the reasons for resorting to the emergency procedure; the grounds for seeking authorization to intercept; and, the persons and places sought to be intercepted. In our view, this is the minimum record necessary.

RECOMMENDATIONS

52. That section 178.15 be amended by the addition of subsection (6) as follows:

> **The admissibility of evidence acquired as a result of an order obtained under this section is not affected by the fact that the electromagnetic, acoustic, mechanical or other device was installed prior to the obtaining of the order, where the order under this section was obtained in relation to the offence under subsection 247(1) (kidnapping) and no private communications were acquired through use of the device until the order was obtained.**

53. That an application for an emergency authorization under section 178.15 shall be made in writing or by telephone or other means of telecommunication and there shall be a record including: a statement of the reasons why an authorization could not, with reasonable diligence, be obtained under section 178.13; the facts relied upon to justify the belief that an authorization should be given, together with particulars of the offence; the persons whose private communications it is sought to intercept; and, the places of interception.

202. *R.* v. *Gamble and Nichols* (1978), 40 C.C.C. (2d) 415 (Alta. S.C. A.D.).

203. *Id.*, pp. 423-4.

V. Remedies

A. Admissibility of Evidence of Other Offences

It is the nature of electronic surveillance that evidence of other offences than those set out in the authorization may be intercepted. This is particularly the case in a system which does not require minimization as it relates to the subject-matter of the conversation. There are several problems which arise in this area as follows:

1. Ought the law distinguish between unanticipated or "windfall" evidence and evidence which could be foreseen?

2. In either case, do we need a system for obtaining authorization for the new offence or other offences?

3. How do we treat the admissibility of such evidence?

4. What about evidence of offences for which no authorization could have been obtained?

Let us consider first the question of windfall evidence. There is an analogy in this respect to search and seizure, where it is generally accepted that evidence is lawfully (constitutionally) seized if it is uncovered during a lawful search for other evidence in circumstances under which the finding of the new evidence was unanticipated. This is simply a particular application of what is called the plain view doctrine in United States Fourth Amendment jurisprudence.[204]

Where the evidence is unanticipated, no serious policy issues arise. No privacy interest is seriously threatened, since the invasion of privacy has already been legitimately authorized for other reasons.

The integrity of the legislative scheme is also not endangered by permitting the authorities to use such evidence. To the contrary, to refuse to use the evidence could have serious effects on the perception of the legitimacy of the scheme, as indicated in *United States* v. *Cox*.[205]

Questions of policy arise when the evidence of other offences is anticipated. In such circumstances, privacy interests are at stake and the integrity of the legislative scheme is threatened. The underlying assumption of wiretap legislation is a reluctant acceptance that in certain carefully defined circumstances, serious invasions of privacy

204. *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971); *Texas* v. *Brown*, 103 S.Ct. 1535 (1983); The doctrine is recognized at common law: *Chic Fashions (West Wales) Ltd.* v. *Jones*, [1968] 2 Q.B. 299 (C.A.).

205. *United States* v. *Cox*, 449 F.2d 679 (1971) (10th Cir.), pp. 686-7.

are to be countenanced. At the heart of the scheme is that such serious intrusions will only be permitted for the investigation of certain offences. Ideally, the offences for which wiretapping will be permitted have been selected only after a most delicate balancing of interests. The legitimacy of the entire process is threatened if an authorization is obtained in relation to one offence as a cover for other offences, which may or may not be offences for which an authorization could be obtained (subterfuge interceptions).

The primary control in this area must either be judicial, through the application procedure, or at the stage of admissibility of evidence. Unfortunately, there is no basis for any confidence that the necessary control can be achieved at the authorization application stage; thus, we believe that the application procedure must be structured so that the necessary control can be exercised at the stage of admissibility of evidence. In our view, the only effective way to guard against subterfuge interceptions is to require a showing of good faith at the *voir dire* during the trial whenever it is sought to introduce evidence at the trial of offences not named in the authorization. This additional burden on the Crown will encourage complete disclosure at the application stage, since there will be an incentive to obtain an authorization which names all the offences for which an authorization can be obtained. It will also discourage attempts to obtain authorizations as a means of obtaining evidence of other offences for which an authorization could not be obtained. In our view, good faith in this context would include the following:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception (this could be an important clue to the true motives and good faith of the authorities — for example, disclosure that it was intended to pass on information to tax authorities may shed light on the real focus of the investigation[206]);

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because: (i) the grounds for suspicions were not strong enough to meet the statutory test; and (ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

206. See the judgment of Anderson J.A. in *R.* v. *Chambers*, *supra*, note 107.

In our view, these are reasonable safeguards and not out of line with the decisions of the Supreme Court of Canada in *R.* v. *Commisso*.[207] Although that case turned primarily on the interpretation of *Code* subsection 178.16(3.1), both the majority and the dissent touched on the question of good faith. In his dissent, Dickson J. stated that an authorization is obtained in bad faith "where the police, although investigating both the specified and unspecified offences, were primarily interested in the unspecified offence for which they could not get an authorization."[208]

In our view, failure to meet the statutory good-faith test can be considered grounds for exclusion of the evidence. Failure of a showing of good faith is in essence evidence of an attempt to defeat the legislative scheme and privacy safeguards. To admit the evidence in such circumstances could bring the administration of justice into disrepute.

RECOMMENDATIONS

54. That where the prosecution seeks to adduce primary evidence obtained by means of an authorization at the preliminary inquiry or trial of offences none of which are named in the authorization, the judge shall conduct a *voir dire* for the purpose of determining whether the interception of evidence of such offences was done in good faith.

55. That for the purposes of Recommendation 54, "good faith" means:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception;

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because

(i) the grounds for suspicions were not strong enough to meet the statutory test,

(ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

---

207. *R.* v. *Commisso* (1983), 7 C.C.C. (3d) 1 (S.C.C.).

208. *Id.*, p. 11.

56. That where he is not satisfied that the interception of other offences was done in good faith, the judge shall exclude primary evidence and may exclude evidence shown to be derivative, where he is satisfied that to permit such evidence to be adduced would bring the administration of justice into disrepute.

B. For Breach of the Statutory Scheme

(1) Introduction

As part of the Police Powers Project, the Law Reform Commission has been concerned with appropriate sanctions, where the rules as they may be enacted in legislative form, are not complied with by the agents of the state. Enactment of subsection 24(2) of the *Canadian Charter of Rights and Freedoms* has focused attention on exclusion of evidence as the appropriate enforcement mechanism. Not unnaturally, the Commission has considered variants on the rule set out in subsection 24(2) as the test for exclusion of evidence, and rules have been derived which can be found in the Reports on *Questioning Suspects*[209] and *Investigative Tests*.[210] As is apparent from the ensuing discussion, the test for exclusion of evidence in the area of electronic surveillance is different, being both stricter in some respects and more liberal in other respects, particularly as regards defects in the application procedure. It may be that, at a later date, an effort will be made to achieve a uniform rule, but at this stage we are satisfied that the different exclusionary rule for electronic surveillance can be justified.

In the first place, it must be recognized that unlike other aspects of the Police Powers Project, when we came to review electronic surveillance there was already in place a strict exclusionary rule with respect to primary evidence (the communication itself) and a looser exclusionary rule with respect to derivative evidence, not unlike the rule in subsection 24(2) of the Charter. It is to be remembered as well that this is perhaps the most intrusive investigative device which Parliament has authorized. When it was enacted, it was recognized that Part IV.1 gave the police expanded powers of investigation which, however, placed a substantial responsibility on the law enforcement agencies to comply fully. As a result, specialists have arisen within the police and prosecution to prepare the applications and carry out the authorizations, and it is not unreasonable to expect a high level of compliance. The often heard criticism of the exclusionary rule, namely, that it punishes the "cop on the beat" who is required to act quickly in emergency situations and who may not have the necessary training in the law, simply does not apply in this context.

---

209. Law Reform Commission of Canada, *Questioning Suspects*, [Report 23] (Ottawa: Minister of Supply and Services Canada, 1984).

210. Law Reform Commission of Canada, *Investigative Tests: Alcohol, Drugs and Driving Offences*, [Report 21)] (Ottawa: Minister of Supply and Services Canada, 1983).

Finally, the essence of the procedure for legalized wiretapping requires invocation of the court's process and justifies the court's taking a significant role in monitoring compliance through the only meaningful tool available, control over the trial process and admissibility of evidence. Seen in this context, even the absolute exclusionary rule is not much different from the modified "bring the administration of justice into disrepute" rule proposed in the other Commission Reports, since it is virtually implicit that failure to comply with a court order has an element of disrespect for the administration of justice.

(2) The Problem of Exclusion Generally

Under this heading we deal with the admissibility of evidence. Certain special rules have already been dealt with because of the important and specific policy considerations unique to those areas, namely, foreign interceptions (Recommendations 11 to 13) and interception of other offences (Recommendations 55 and 56).

Here, we deal more specifically with the problem of exclusion of evidence as the primary mechanism for enforcement of the legislative scheme. While in this discussion we deal briefly with the exclusionary rule generally, as it is formulated in current section 178.16 of the *Criminal Code*, the real problem dealt with is the impact of a review procedure. To focus the debate, we have set out two alternatives to the definition of substantive defect in the application. It will be recalled that we recommend exclusion of evidence as the remedy for a substantive defect in the application. The two alternative formulations delineate the parameters of the exclusionary rule in the review context. Those alternatives which can be described as "A": the rule of absolute exclusion, and "B": the good-faith exception rule, are as follows:

Alternative "A": Absolute Exclusion

That a substantive defect in the application means:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed; or

(b) reasonable and probable grounds did not exist to believe that a targeted offence was being committed by a person provided for in the authorization; or

(c) any other grounds from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

Alternative "B": Good-Faith Exception

That a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed; or

(b) reasonable and probable grounds did not exist to believe that a targeted offence was being committed by a person provided for in the authorization; or

(c) any other grounds from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

To focus the issues further, we include a discussion of the recent decision of the United States Supreme Court in *United States* v. *Leon*,[211] where that court for the first time recognized a good-faith exception to the Fourth Amendment exclusionary rule in circumstances of great relevancy to this Paper — namely, good-faith reliance on a judicial warrant. We then explore the rationale for an exclusionary rule, and conclude with our recommendations in this area. Let it be said that these are difficult policy choices and we favour that remedy which best balances the competing interests. The decision in *Leon* is an attempt at striking such a balance in the American context. Subsection 24(2) of the Charter is also an attempt to strike an appropriate balance in the context of the violation of constitutional protections. As will be seen, in the end we recommend very little change to the present exclusionary rule in Part IV.1; most of our recommendations are aimed at clarifying the procedure and the rules.

At present under Part IV.1 of the *Criminal Code*, the exclusionary rule operates in several respects:

(a) where there has been inadequate notice *per* subsection 178.16(4);

(b) where there is no authorization and no consent, that is, an unlawful interception;

(c) where there is an authorization, but the interception is not made in compliance therewith, that is, of a person's communication not provided for in the authorization;

(d) where the authorization is, in effect, reviewed and set aside.

These all apply to primary evidence, that is, the actual communication; a different test applies to derivative evidence.

Our recommendations would alter situations (a) (notice) but we do not propose any change in (b) (unlawful interception and no consent), and (c) (noncompliance with authorization). Since we propose a change in the sanctions for notice, a discussion is set out below. We should, however, briefly discuss at this point an issue concerning compliance with the authorization. Prior to the decision of the Supreme Court of Canada in *Lyons* v. *The Queen*[212] there was some uncertainty as to the scope of the prerequisite for admissibility in paragraph 178.16(1)(*a*) that the "interception" be "lawfully made." the majority judgment in *Lyons* deals with this problem in a wholly satisfactory way which respects both the principles of privacy and effective law enforcement.

In *Lyons*, Estey J. for the majority held that the process of interception is a single undertaking carried out under an authorization which cannot be segmented into legally

211. *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

212. *Supra*, note 123.

consequential and inconsequential steps. Thus, for example, an unlawful act in the installation of the device could taint the legality of the interception. The Ontario Court of Appeal had come to a similar conclusion in two recent cases: *R.* v. *Papalia*[213] and *R.* v. *McCafferty*.[214] It was also held, however, that "lawfully made" in paragraph 178.16(1)(*a*) does not mean in compliance with all laws, but rather in compliance with Part IV.1. Thus, surreptitious entry for installation of a device, if done to implement the authorization, would be lawful. If done, however, before the authorization was granted, perhaps under cover of a search warrant (as in *McCafferty*), then the interception would not have been done pursuant to an authorization and would not have been lawfully made, even if no actual recordings were done until after the authorization was obtained.

C. Notice under Subsection 178.16(4)

The present provisions of Part IV.1, specifically subsection 178.16(4), require that the prosecution give the accused notice that it intends to adduce a private communication. The notice must be "reasonable" in time and contain a statement as to the time, place and date of the private communication. As well, a transcript must be provided if the tape recording is to be played; otherwise, a statement setting forth full particulars is required. In the absence of any of this material, the evidence is inadmissible. The notice provision, by its terms, applies to a lawfully intercepted private communication which seems only to refer back to the alternative in paragraph 178.16(1)(*a*), namely, evidence of private communications being admissible where the interception was lawfully made, rather than to paragraph 178.16(1)(*b*), which permits admission of evidence no matter how obtained with consent of one of the parties to the communication, not necessarily the accused. The notice requirements of subsection 178.16(4) essentially perform a discovery function and only a tenuous privacy function. In our view, the discovery function applies whether the evidence is adduced under either paragraph 178.16(1)(*a*) or (*b*). To date, however, case-law has held that notice is not required where the evidence is adduced with the consent of one of the parties.[215] In our view, there is no adequate rationale for this distinction. On the other hand, the scheme of the legislation is that the penalty for defective notice is exclusion of evidence. This seems a drastic sanction for provisions designed to serve primarily a discovery function. In our view, exclusion of evidence should be reserved for serious breaches of the provisions; the primary control mechanism in this area should be towards enforcing compliance. If the failure to comply with the notice provisions results in unreasonable delay, sanctions are available under the *Canadian Charter of Rights and Freedoms*.[216]

213. *R.* v. *Papalia* (1984), 13 C.C.C. (3d) 449 (Ont. C.A.).

214. *Supra*, note 147.

215. See: *R.* v. *Banas and Haverkamp* (1982), 65 C.C.C. (2d) 224 (Ont. C.A.); *R.* v. *McDonald and Tondu* (1981), 60 C.C.C. (2d) 336 (Alta. C.A.).

216. Particularly the guarantee to a trial within a reasonable time in paragraph 11(*b*).

Of course, as set out above, the notice requirements would be extended to require the Crown to provide a copy of the authorization or renewal and the material referred to in section 178.14 which has not been ordered withheld by a court. The same reasoning applies, however, as failure to comply would not lead to exclusion of evidence, but only to sanctions designed to enforce compliance.

In the past, some question has arisen as to the application of section 178.16 to bail hearings. In a recent decision, *R.* v. *Kevork*,[217] Ewaschuk J. was of the view that the wording of paragraph 457.3(1)(*e*), which permits the justice to dispense with the strict pre-conditions as to admissibility of evidence, meant that section 178.16 did not apply at bail hearings. Whether or not this is a correct interpretation of sections 457.3 and 178.16, we are of the view that evidence of intercepted private communications or evidence derived therefrom ought to be admissible at bail hearings without a strict inquiry into the lawfulness of the interception, provided it was apparently made under an authorization or with the consent of a party. In this respect we note the proposed amendment to subsection 457.3(1) of the *Code* in subsection 85(1) of Bill C-18 (as passed by the House of Commons on April 24, 1985) which will add a new paragraph (*d*.1) as follows:

> the justice may receive evidence obtained as a result of an interception of a private communication under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, subsection 178.16(4) does not apply to such evidence; ....

However, the wording of this amendment might be improved by making it clear that it was intended to cover both the communication itself and derivative evidence.

D. Substantive Defect in the Application

The real policy problem presented with respect to admissibility of evidence concerns the problem of review of the application for the authorization.

Simply put, the dilemma is this: What is the justification for excluding evidence where the evidence has been gathered by the police acting under, and in accordance with, a judicial mandate? If the point of the legislative scheme is to require judicial scrutiny prior to the interception, what are the compelling reasons for excluding evidence where a judge has passed on the merits of the application and, in the exercise of a judicial function, has authorized the intrusion? There is, of course, one clear case where the protection envisaged by the legislative scheme is subverted by the police conduct. This is the situation covered by alternative "B." The authorizing judge is really not in a position to assess properly the merits of the application and thus protect against

217. *R.* v. *Kevork* (1984), 12 C.C.C. (3d) 339 (Ont. H.C.J.).

unwarranted intrusion if he has been misled, intentionally or recklessly, as to the true state of affairs. In such circumstances, as in the *Gill* case,[218] the need for exclusion of evidence to deter such conduct is clear.

The more difficult case is where the authorities have made a proper application, relied upon the judge's determination that it is sufficient, acted in good-faith reliance upon the authorization only to find the evidence excluded because another judge determines that, for example, the material did not disclose the requisite reasonable and probable grounds.

The distinction between the two cases was considered by the Supreme Court of the United States in *United States* v. *Leon*,[219] where White J. speaking for the majority of the court carved out a good-faith exception to the rule of absolute exclusion of evidence obtained in violation of Fourth Amendment rights. The majority accepted that the requisite probable cause did not exist to issue a search warrant but held that evidence received pursuant to that warrant was nevertheless admissible. White J. considered that the rationale of the exclusionary rule was future deterrence of wrongdoing by the police, and that the rationale was not sufficiently strong in the case of good-faith reliance on a warrant.

Justice White considered at some length the rationale for the exclusionary rule, in particular with the concept of deterrence, and concluded that "[i]f exclusion of evidence obtained pursuant to a subsequently invalidated warrant is to have any deterrent effect, therefore, it must alter the behavior, of individual law enforcement officers or the policies of their departments," and further, "that suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in these unusual cases in which exclusion will further the purposes of the exclusionary rule."[220]

The protection offered to privacy rights by Part IV.1 of the *Criminal Code* is similar to the protection offered by the Fourth Amendment (and its Canadian equivalent, section 8 of the *Canadian Charter of Rights and Freedoms*). The United States Supreme Court has determined that exclusion of evidence is not the appropriate remedy to protect those constitutional rights in certain circumstances when balancing the costs (essentially, acquitting the guilty) against the benefits (deterrence of future violations of the Fourth Amendment). What then are the arguments against the good-faith exception?

As might be expected, there was a vigorous dissent by Mr. Justice Brennan (Marshall J. concurring). He had foreseen this development in the shift in the courts' approach to Fourth Amendment issues over the previous ten years. Moreover, a debate has raged in the literature for at least that period over a good-faith exception, fueled most recently by the decision in *United States* v. *Williams*[221] where the United States Court of Appeal from the Fifth Circuit sitting *en banc* carved out a wide good-faith exception.

218. *Supra*, note 116.

219. *Supra*, note 211.

220. *Id.*, p. 3419.

221. *United States* v. *Williams*, 622 F.2d 830 (1980), cert. den. 449 U.S. 1127 (1981).

Justice Brennan in his dissent takes a much broader view of the purpose of the exclusionary rule. He does not see it as resting principally on a deterrence theory.[222]

Justice Brennan rejects the narrow deterrence theory, moreover, because of the impossibility of proof one way or another. As he says, quoting Justice Stewart in *Faretta* v. *California*,[223] "[p]ersonal liberties are not rooted in the law of averages."[224] On the other hand, he minimizes the costs of the exclusionary rule, pointing out that the evidence outside that subject to exclusion by reason of Fourth Amendment violation, would likely be sufficient to lead to a conviction.[225] Justice Brennan does, however, support an institutional deterrence theory which proposes that the demonstration "that our society attaches serious consequences to violation of constitutional rights is thought to encourage those who formulate law enforcement policies, and the officers who implement them, to incorporate Fourth Amendment ideals into their value system."[226]

Dealing specifically with the warrant question, Justice Brennan sees dangers in the good-faith doctrine in that there may well be a decreasing incentive for both police and magistrates carefully to prepare and consider applications.

Justice Stevens in his dissent focuses on the purposes of the Fourth Amendment and on an aspect of the debate seemingly overlooked; that is, that the historical roots of the Fourth Amendment are in the abuse of the warrant procedure and the desire of the framers of the Constitution to protect against general warrants and writs of assistance. Historically, "the paradigm of an abusive search was the execution of a warrant not based on probable cause."[227] He sees the exclusionary rule as designed to prevent violation of the Fourth Amendment and the good-faith exception as doing "grave damage to that deterrent function."[228] He also expresses concern over the concept of the courts relinquishing responsibility for constitutional violations.

Thus, we have the two sides of the debate presented in what may be a pivotal constitutional case in the United States where there has been experience with an absolute exclusionary rule for almost twenty-five years in state prosecutions[229] and almost seventy years in federal prosecutions.[230] It is apparent that an examination of that experience should prove useful in the attempt to determine the appropriate rule in the Canadian wiretap context. While it must be borne in mind that the debate in the United States is in a constitutional context involving the enforcement of a constitutional guarantee, this does not necessarily diminish its relevance. Privacy, whether a right of constitutional

222. *Supra*, note 211, pp. 3436-7.
223. *Farena* v. *California*, 422 U.S. 806 (1975).
224. *Id.*, p. 834.
225. *Supra*, note 211, p. 3439.
226. *Id.*, p. 3443.
227. *Id.*, p. 3453.
228. *Id.*, p. 3454.
229. Since *Mapp* v. *Ohio*, 367 U.S. 643 (1961).
230. Since *Weeks* v. *United States*, 232 U.S. 383 (1914).

dimension in law, is certainly increasingly perceived as an important, if not fundamental, right in a modern society. Respect for privacy and restraint on intrusion into legitimate privacy interests underlie much of the work in the Police Powers Project, particularly when considering the reach of such an intrusive device as electronic surveillance.

To start with, then, what is the foundation for an exclusionary rule?

(a) *It is mandated by the Constitution*. This theory developed in the United States on the basis that use of documents seized in violation of the Fourth Amendment would violate the Fifth Amendment guarantee against self-incrimination.[231] This is not a theory which is now generally accepted.[232] It is, however, a theory which has some impact in the Canadian context where our *Canadian Charter of Rights and Freedoms* contains an explicit, if limited, rule of exclusion in subsection 24(2). On this theory, exclusion of wiretap evidence would be justified *if* the accused's constitutional rights were violated *and* the test in subsection 24(2) were met. Certainly, good faith on the part of the authorities is an important consideration in the "all the circumstances" equation.[233]

Any wider or different exclusionary rule must therefore rest on different foundations. It is necessary to explore these for two reasons: first, it is not clear what violations of the statutory wiretap regime are of constitutional impact and it is even less clear when admissions of evidence would bring the administration of justice into disrepute; second, constitutional violations can be expected to take care of themselves. No special legislative mechanisms are required. While it must be borne in mind that even for constitutional violations, Parliament has adopted a far more diluted test than one of absolute exclusion, this does not prevent the adoption of the same or a different rule if its adoption can be justified on another basis.

(b) *Exclusion to preserve the integrity of the government and the courts*. Under this theory, exclusion is required to prevent the government from receiving the aid of the judiciary in giving effect to a Fourth Amendment violation and to prevent the court from committing a second Fourth Amendment violation. Again, while this is not a theory given much credence in the United States,[234] it has relevance to the Canadian debate and in fact answers some of the exclusion problems. In the wiretap context, the issue can be reformulated as follows: Would the court, by admitting the evidence, be party to the commission of a criminal offence? This was a motivating force behind the exclusion of evidence in the case of *R.* v. *Stewart*,[235] even though on its face the regulation did not call for exclusion. Although the normal rule in Canada is that illegally obtained evidence is admissible, that

231. *Supra*, note 229.

232. Potter Stewart, "The Road to *Mapp* v. *Ohio* and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases" (1983), 83 *Colum. L. Rev.* 1365, p. 1381.

233. See: *R.* v. *Simmons*, *supra*, note 86; *R.* v. *Rao*, *supra*, note 46.

234. *Supra*, note 232, pp. 1382-3.

235. *R.* v. *Stewart* (1981), 60 C.C.C. (2d) 407 (Ont. C.A.).

rule does not touch the situation where "the very use or disclosure of the evidence in the course of the trial was unlawful"[236] in which case Parliament's intent must have been exclusion of the evidence.

Admittedly there is a certain artificiality to this foundation in the law reform context since it would be open to the reformers to distort the exclusionary rule by redefining the offences. However, with this borne in mind, what aspects of the regime does this basis for an exclusionary rule encompass? For our purpose, this requires an examination of the exception from liability by subsection 178.2(2) for the disclosure offence created by subsection 178.2(1):

> (2) Subsection (1) does not apply to a person who discloses a private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof or who discloses the existence of a private communication
>
> (*a*) in the course of or for the purpose of giving evidence in any civil or criminal proceedings or in any other proceedings in which he may be required to give evidence on oath where the private communication is admissible as evidence under section 178.16 or would be admissible under that section if it applied in respect of the proceedings;
>
> (*b*) in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted; ....

This then relates back to paragraph 178.16(1)(*a*) and the requirement that the interception was lawfully made, which in turn leads to section 178.11 which gives the parameters of lawful interception. For the purposes of this discussion, that involves two situations: consent interceptions (paragraph 178.11(2)(*a*)), and authorized interceptions (paragraph 178.11(2)(*b*)). It is the latter which is most important; it provides that the interception offence is not committed by:

> ... a person who intercepts a private communication in accordance with an authorization or any person who in good faith aids in any way a person whom he has reasonable and probable grounds to believe is acting with any such authorization; ....

Thus, exclusion of evidence is mandated to avoid the commission of an offence where the interception was not made in accordance with the terms of an authorization. This is the present Canadian position[237] which we do not propose to change. Rather, as indicated *supra*, this rule will remain. It should be noticed that good-faith interception in accordance with the authorization does not exempt from liability the interceptors, only persons, such as telephone company employees, who assist the interceptors in the interception. Accordingly, there is no room for a good-faith exception to the "in accordance with the terms of the authorization" admissibility requirement.

On the other hand, this analysis does not really answer the problem of review of the authorization. It would, of course, be possible to create the fiction that if there is

---

236. *Id.*, p. 437.

237. See: *R.* v. *Welsh and Iannuzzi (No. 6)*, *supra*, note 31; *R.* v. *Niles*, *supra*, note 163.

a substantive defect in the application, then the authorization is set aside,[238] so that in law, the officers were not acting in accordance with the terms of the authorization and therefore were acting illegally *per* subsection 178.11(1). However, this kind of retroactive imposition of liability is offensive to ordinary notions of justice even leaving aside nice questions of *mens rea* and the application of paragraph 11(*g*) of the *Canadian Charter of Rights and Freedoms*. A much more satisfactory approach is to address the review problem directly by acknowledging the fact that the authorities did intercept in accordance with an authorization, which at that time was valid, and to ask whether notwithstanding this fact and notwithstanding that they committed no offence in doing so and would commit none by the act of introducing the evidence obtained in court, there is some other basis for exclusion of evidence where there was a substantive defect in the authorization.

Under the theory of exclusion as a required remedy for enforcement of the scheme, exclusion of evidence is required in the Fourth Amendment context to ensure that the government does not violate the Fourth Amendment. It is justified then only if other adequate remedies of enforcement do not exist.[239] This then is the focus of the deterrence debate. Herein lies the justification for the good-faith exception. It is in this context that the rationale, if any, for exclusion of evidence on any basis is warranted for defects in (or violation of) the authorization application procedure. This requires examination of the costs and benefits of an exclusionary rule, and of alternative remedies.

It should be pointed out that, as in the Fourth Amendment exclusionary rule debate, there is one given — namely, it is a good thing for the authorities to comply with the statutory scheme (as it is a good thing for the authorities in the United States to comply with the Fourth Amendment). That one seeks remedies of any kind for violations of the scheme is part of the commitment to ensuring that it remains an effective protection against violations of the scheme and of legitimate privacy interests. Two questions must be asked:

1. What are the purposes of any remedy?

   (a) Specific deterrence: deterring the particular officer from repeating the same violation of the legislative scheme.

   (b) General deterrence: deterring other officers from repeating the same violation of the scheme.

   (c) Systemic deterrence: encouraging the authorities to put in place mechanisms to prevent future violations.

2. What are the alternative remedies to exclusion of evidence?

238. *Wilson* v. *The Queen*, *supra*, note 167.

239. *Supra*, note 232, p. 1384.

(1) Tort Remedy

One alternative to exclusion of evidence which would operate to secure compliance would be to put in place a statutory tort remedy, allowing the victim of an improperly authorized interception to sue the authorities. The American literature, however, almost uniformly admits its ineffectiveness in securing compliance.[240]

In our view, many of the same considerations would make a statutory tort remedy an ineffective means of securing compliance to the Part IV.1 process. Moreover, certainly to date, civil remedies have not been the preferred route either for remedying violations or for securing enforcement. Part I.1 of the *Crown Liability Act*,[241] and section 178.21 of the *Criminal Code* provide for damage awards for unlawful interceptions or disclosures either by agents of the Crown or private persons. We are unaware of any action (successful or otherwise) against any officer for any activity related to electronic surveillance, notwithstanding that, it is argued, when evidence is excluded under paragraph 178.16(1)(*a*), a possible tort action would lie.

(2) Criminal Liability

Another alternative to exclusion of evidence would be to widen the criminal liability by creating offences designed to ensure compliance with the application procedure. Again, experience would indicate that this is not an effective remedy for compliance.[242]

It is notoriously difficult to obtain convictions of police officers even in cases in which outrageous conduct is alleged. This is not to pass judgment on the validity or not of these allegations, but the institutional barriers including proof of *mens rea*, proof beyond a reasonable doubt and reliance on brother officers to provide evidence, all work against threat of criminal prosecution as a realistic enforcement mechanism. Once again, experience under Part IV.1 bears this out. Paragraph 178.22(3)(*a*) requires the annual report of the Attorney General or Solicitor General to set forth "... the number of prosecutions commenced against officers or servants of Her Majesty in right of Canada or members of the Canadian Forces for offences under section 178.11 or section 178.2; ...." We could find no report of any such prosecution. Further, we are unaware of the prosecution of any member of a municipal or provincial police force.[243]

---

240. William J. Mertens and Silas Wasserstrom, "The Good Faith Exception to the Exclusionary Rule: Deregulating the Police and Derailing the Law" (1981), 70 *Geo. L.J.* 365, pp. 406-10; Stewart, *supra*, note 232, pp. 1387-8; William A. Schroeder, "Deterring Fourth Amendment Violations: Alternatives to the Exclusionary Rule" (1981), 69 *Geo. L.J.* 1361, pp. 1386-96.

241. *Crown Liability Act*, R.S.C. 1970, c. C-38, as amended by S.C. 1973-74, c. 50, s. 4.

242. Schroeder, *supra*, note 240, pp. 1396-8; Stewart, *supra*, note 232, pp. 1386-7.

243. While we have recommended the creation of an offence for unauthorized surreptitious entry, we admit that this is to some extent symbolic but reflective of the seriousness with which we view this particular intrusion.

(3) Extrajudicial Controls

Under this heading might be considered independent review boards and internal disciplinary procedures. To the extent that their mechanisms would depend on initiation of action by citizens, they suffer from the same defects as the remedies considered above. While an independent review board could be founded on referrals by trial judges, it is unlikely that this would represent a sufficient enforcement mechanism. If the manner in which the application is made is legally irrelevant to the trial, then there would be no incentive to uncover violations of the application procedure. To the contrary, with the increasing pressure on the courts brought about by case-load and delays, there is a real disincentive on the part of the judge to embark on legally irrelevant lines of inquiry, and no particular incentive on the part of the accused or the Crown to make the inquiry. Internal controls suffer from many of the same disincentives. "Police officers often ignore serious misconduct by fellow officers and Courts rarely notify police administrators of misconduct by their officers."[244]

(4) Exclusionary Rule

This then leaves consideration of the exclusionary rule; however, only within a very narrow compass, namely, enforcement of compliance with the application procedure by exclusion of evidence in cases of substantial noncompliance. We have already set out the two alternative models, one based on automatic exclusion for failure to comply, and one based on exclusion only where there is not good-faith compliance. The costs of exclusion previously referred to include inaccurate fact-finding — normally resulting in: the guilty going free; otherwise meritorious charges being dropped or plea bargained for inadequate sentence; and, disrespect for the law as a result of the perception that the guilty are set free or inadequately dealt with.

A significant criticism of an exclusionary rule is that, like the other proposed remedies, it does not in fact deter misconduct.

First, let us give consideration to the costs. While many studies have been done in an attempt to quantify the costs in terms of lost or dropped prosecutions as a result of the Fourth Amendment exclusionary rule, the studies are probably inconclusive.[245] Advocates of the absolute exclusionary rule tend to minimize the costs.[246] Advocates of its abolition tend to magnify those costs. It has, however, been pointed out that the impact on serious cases such as murder is exaggerated and that in most instances other

244. Schroeder, *supra*, note 240, p. 1401. See also Stewart, *supra*, note 232, p. 1388.

245. See: Thomas Y. Davies, "A Hard Look at What We Know (and Still Need to Learn) about the Costs of the Exclusionary Rule: The NIJ Study and Other Studies of 'Lost' Arrests" (Summer, 1983), 3 *American Bar Foundation Research Journal* 611; Bradley C. Canon, "Ideology and Reality in the Debate over the Exclusionary Rule: A Conservative Argument for Its Retention" (1982), 23 *S. Tex. L.J.* 559; Mertens and Wasserstrom, *supra*, note 240; Schroeder, *supra*, note 240, pp. 1382-5.

246. Stewart, *supra*, note 232, p. 1394.

evidence is available.[247] This is not to minimize the seriousness of these costs but only to put them in focus.[248] Certainly, some of the recent case-law under the Charter have raised the same considerations.[249] Similarly, attempts to quantify the deterrent impact of the rule on police behaviour have been inconclusive.[250] Ultimately, this aspect of the debate must proceed on the basis of intuitive arguments.[251]

Some of these arguments may lose their force in the area of electronic surveillance applications because of the way these applications are prepared. These are not quick on-the-spot decisions, but rather the product of scrutiny at various levels, until passed on by a designated prosecutor with some expertise in the area. Thus, court decisions, for example, on what constitutes reasonable grounds or lack of alternative investigative means, would impact on subsequent applications, and prevent future improper applications. As well, judges hearing the applications would become aware of the decisions.

Moreover, none can doubt the reality of an exclusionary rule. Unlike criminal or civil sanctions, judges do exclude evidence and police do modify their procedures in response.[252]

Further, exclusion of evidence following a judicial hearing serves the interests of developing guidelines for the authorizing judge as to what in law constitutes compliance with the application conditions such as reasonable cause, lack of alternative investigative procedures, and so forth, so as to prevent future violations.[253]

Advocates of the good-faith exception to the exclusionary rule argue that most of these interests are served by a rule which allows for admission of evidence where the authorities have not acted wilfully or recklessly to avoid the strictures of the law, without the high cost which is exacted by an absolute exclusionary rule. In effect there is a certain balancing test. The rationale seems particularly strong when police have acted in good-faith reliance on a warrant (or authorization, in the wiretap context). Schroeder stated the following:

> Special problems involving the use of a good faith test arise when an officer seeks and obtains a search warrant. A search conducted *in accordance with the terms of the warrant* necessarily involves good faith, unless the police misrepresent facts to the magistrate in order to obtain the warrant. Nevertheless, the attorney preparing the affidavit and applying for the warrant or the magistrate issuing the warrant frequently makes errors that might

247. Mertens and Wasserstrom, *supra*, note 240, pp. 445-6.

248. See Schroeder, *supra*, note 240, p. 1384.

249. For example, *R.* v. *Collins* (1985), 5 C.C.C. (3d) 141 (B.C. C.A.).

250. See: Dallin H. Oaks, "Studying the Exclusionary Rule in Search and Seizure" (1970), 37 *U. Chi. L. Rev.* 665; Schroeder, *supra*, note 240, pp. 1378-82; Davies, *supra*, note 245, especially pp. 627-9.

251. See Schroeder, *supra*, note 240, p. 1384.

252. See Mertens and Wasserstrom, *supra*, note 240, pp. 400-1.

253. Advocates of the Fourth Amendment exclusionary rule consider this an important purpose of the rule. See: Mertens and Wasserstrom, *supra*, note 240, pp. 401-6; Wayne R. LaFave, *Search and Seizure* St. Paul, Minn.: West Publishing, 1978), vol. 1, 1984 Pocket Part at pp. 13-8; Stewart, *supra*, note 232, pp. 1400-1.

> invalidate an entire search. When the police have dutifully applied to a judge or a magistrate for a search warrant, and have executed the warrant in strict conformity with its terms, exclusion of the evidence thus obtained can have no possible deterrent effect on future police conduct. Of course, exclusion of the evidence might improve the decisions of those magistrates who issue warrants pro forma or who lack the ability to evaluate intelligently the evidence before them. Even conscientious and well-trained magistrates occasionally make mistakes, however, and in such cases exclusion has absolutely no deterrent value. Thus, it makes sense to retain the exclusionary rule only for warrantless searches and those searches made on the authority of warrants based on perjured testimony or on evidence so scant that no reasonable magistrate could have believed it. This would encourage bona fide resort to warrants while also protecting individuals against abuse of warrant procedures.[254] [Emphasis added]

The debate, however, is not all one way on the good-faith exception, and arguments have been advanced to support the broader exclusionary rule.[255]

One problem that is mentioned is that of judge shopping; this could be considered a serious potential weakness of a good-faith rule of the type outlined in our alternative "B." The legitimacy of that alternative depends on the neutrality of the issuing judge to safeguard against improper applications. Judge shopping implies that the prosecutor is able to choose the judge who will determine the validity of the application for an authorization and that this is done because the judge is partial, "Crown/police oriented" or perhaps merely inexperienced and likely to be overwhelmed by the application and the expertise of the police and the designated agent. Thus, in case of an application of doubtful merit or of great importance, the risk of refusal is minimized. In its more positive aspect, a particular judge may be selected because of his expertise, to ensure that everything is in fact in order so as to minimize future difficulties. This would be important where there is a perception that the litigation stemming from the authorization will be particularly hard fought and the material closely scrutinized.

A disadvantage of the secrecy provisions is that, on the one hand, not only is it impossible really to quantify judge shopping, but on the other hand, that very secrecy encourages the perception that it goes on. Ultimately, however, and despite claims to the contrary, we believe that judge shopping rests only on speculation.[256] In its most negative sense it depends on bad faith on the part both of the agent and the judge and we would be loathe to reject a rule, otherwise meritorious, on the basis of this kind of speculation.

This, however, does not take away from the importance of the perception that judge shopping goes on. As we have said, that perception, always present in any *ex parte* proceeding, is reinforced when the proceedings are forever secret and where no record is kept of what occurs. We would not want our proposed regime threatened by

---

254. Schroeder, *supra*, note 240, pp. 1418-9.

255. See, for example, the dissent in: *Unites States* v. *Leon*, *supra*, note 211; Stewart, *supra*, note 232, p. 1403; Mertens and Wasserstrom, *supra*, note 240; LaFave, *supra*, note 253, pp. 11-5.

256. However, see Cohen, *supra*, note 97, pp. 140-3 and references therein, particularly the U.S. *Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance* (1976), pp. 73-4.

the *perception* that judge shopping can undermine its safeguards. Since we recommend that the material used on the application be eventually disclosed to the defence, this should relieve some of the concern. One suggestion that has been made to deal with the problem of this perception is to follow the approach taken in the United States by the Administrative Office of the United States Courts in the Wiretap Report[257] and publish the names of the judges and the number of orders they have granted. This suggestion has been put to persons with whom the Commission has consulted in the past and there has been little enthusiasm for it. Moreover, it is not clear whether this really serves the purposes of avoiding judge shopping.

We would prefer that the problem be dealt with directly, and would hope to see the implementation of administrative rules which put in place a formal rotation system. Under such a system the prosecutor must simply take the judge assigned to do authorizations. This is obviously a system which cannot operate effectively in a small jurisdiction, but in such a jurisdiction the options for judge shopping are simply minimal. We are also aware of systems in some of the larger districts for having a panel of designated judges; provided such judges do not come to feel that they are allied within the prosecution because of the frequency with which they deal with such applications, we feel that such a system, designed to encourage expertise among the authorizing judges, is not inconsistent with our recommendation. We do not, however, feel that it is necessary that this be a formal recommendation.

Then, accepting the criticism of Justice Stewart and the other commentators, but bearing in mind the levels of authority involved in a wiretap application, one may ask, Is the limited good-faith exception as outlined in alternative "B" not the appropriate compromise? Such a test would eliminate the worst abuses and the possibility of judicial inquiry will protect against some improper applications. Some case-law will develop to guide authorizing judges, since an inquiry into good faith requires some investigation of the appropriate standards. The problem that a good-faith exception may place a premium on ignorance can be dealt with by excluding from good faith, reckless failure to comply with the statutory conditions. On balance therefore, *in the area of review of the authorization for substantive defects in the application*, we favour a good-faith exception to exclusion of evidence as the primary enforcement mechanism.

E. Derivative Evidence

Derivative evidence is that evidence, other than the private communication itself, which is obtained as a result of the acquiring of the private communication. Presently, section 178.16 contains a limited exclusionary rule as follows:

> (1) A private communication that has been intercepted is inadmissible as evidence against the originator of the communication or the person intended by the originator to receive it unless

257. *Supra*, note 150.

(*a*) the interception was lawfully made; or

(*b*) the originator thereof or the person intended by the originator to receive it has expressly consented to the admission thereof;

but evidence obtained directly or indirectly as a result of information acquired by interception of a private communication is not inadmissible by reason only that the private communication is itself inadmissible as evidence.

(2) Notwithstanding subsection (1), the judge or magistrate presiding at any proceedings may refuse to admit evidence obtained directly or indirectly as a result of information acquired by interception of a private communication that is itself inadmissible as evidence where he is of the opinion that the admission thereof would bring the administration of justice into disrepute.

In section 178.16, the rule is broadly framed applying to evidence obtained directly or indirectly. Any derivative evidence rule can pose difficult problems such as the following:

(a) If the derivative evidence was obtained from two sources only one of which is tainted, is it excludable?

(b) Upon whom is the burden of showing what evidence is derivative?

(c) Should derivative evidence be subject to automatic exclusion?

(d) Does issuance of a renewal or new authorization break the chain of taintedness?

Some of these issues were considered by Borins Co.Ct.J., in *R.* v. *Samson (No. 6)*.[258] In that case, His Honour found that much of the Crown's case was obtained directly or indirectly from inadmissible primary evidence. He considered that the burden was on the Crown to demonstrate that its evidence was not derivative. Further, it did not matter that the evidence might have been obtained from other sources. The question is, How in fact was it obtained? Evidence obtained from mixed (tainted and untainted) sources was also derivative. Further, he found that evidence obtained pursuant to a subsequent authorization was derivative if the application for the subsequent authorization was based on unlawful interceptions. On the Crown appeal[259] these issues were not dealt with in view of the court's determination that the primary evidence was admissible.

In considering these issues, we can draw on two streams of American experience: firstly, the experience under Title III, specifically section 2515 which provides that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, ... if the disclosure of that information would be in violation of this chapter" and secondly, the "fruit of the poisonous tree" doctrine in Fourth Amendment jurisprudence. As it happens, however, it was the intent of Congress that the "fruit of the poisonous tree" doctrine principles apply to derivative evidence questions under section 2515.[260] Generally speaking, the burden is on the accused to demonstrate on a preponderance of evidence that the prosecution's evidence is tainted by the

258. *Supra*, note 102.

259. *Supra*, note 58.

260. See "The Legislative History of Title III, Senate Report No. 1097," which is Appendix B in David Watt, *Law of Electronic Surveillance in Canada* (Toronto: Carswell, 1979), pp. 378-9.

illegal interception. However, tainted evidence can include interceptions obtained under an order which was itself obtained by use of tainted evidence, and if the original order was tainted, any extensions are automatically tainted.[261]

Difficult questions can arise in applying the so-called attenuation rules, developed under the Fourth Amendment. For example, where the existence of a witness is discovered from an unlawful interception, when is that witness' testimony tainted and therefore inadmissible,[262] and what material is the accused entitled to see in order to meet the burden of establishing the taint?[263]

The recent trend in United States Supreme Court decisions is to cut down the scope of the "fruit of the poisonous tree" doctrine in Fourth Amendment legislation. This, of course, has a direct impact on taint litigation under Title III. The court has done this by extending the attenuation rules. A recent statement of that rule in *Segura* v. *United States*,[264] provides that the evidence is not to be excluded if it is " 'so attenuated as to dissipate the taint.' "

In Canada there are two weak analogies to the poisonous tree doctrine. As is well known, physical evidence obtained as a result of an illegal confession is admissible — the so-called *St. Lawrence*[265] rule. As well, the no-substantial-wrong proviso in subparagraph 613(1)(*b*)(iii) of the *Criminal Code*, which permits dismissal of an appeal notwithstanding errors of law at trial, is a type of attenuation rule. Thus, there is really little Canadian experience to draw upon. In our view, the primary purpose of a derivative evidence rule in the wiretap regime must be to deter wilful failure to comply with the statutory procedures and safeguards. When the wiretap Bill was first introduced the police represented that the optimal use of wiretaps was to gather intelligence, that is, to gather other evidence of criminal activity, not necessarily to use the communications themselves. We would not want to encourage a system whereby unlawful interceptions are made by the police for intelligence-gathering purposes without fear that evidence derived therefrom would nevertheless be inadmissible. This would undermine all the lawful protections of the legislative scheme and bring the administration of justice into disrepute.

On the other hand, we are very concerned to avoid the complexities which seem to be the inevitable product of any derivative evidence rule. In our view, many of the complexities in the United States derive from the rule of automatic exclusion which flows from a finding of taint. For that reason, the courts strain to take the evidence outside the taint rule. If we could therefore give the courts a discretion to exclude evidence and couple it with some simple rules as to what is derivative, then some of these problems would, it is hoped, be avoided.

---

261. See *United States* v. *Giordano*, *supra*, note 171.

262. See *United States* v. *Ceccolini*, 435 U.S. 268 (1978).

263. See *Alderman* v. *United States*, 394 U.S. 165 (1969). Generally, for a detailed discussion of all of these issues in the electronic surveillance field, see Carr, *supra*, note 67, Chapter 6.04.

264. *Segura* v. *United States*, 104 S.Ct. 3380 (1984), *per* Burger C.J., p. 3386.

265. *R.* v. *St. Lawrence*, *supra*, note 79; *R.* v. *Wray*, *supra*, note 8.

F. The Length of Proceedings

Over the years, since the enactment of Part IV.1, concern has been expressed as to the length of proceedings on the *voir dire*. Electronic surveillance is a highly intrusive means of investigation which has necessitated strict controls. As a result, proof of compliance with those controls takes time. As well, the evidence is sometimes highly technical and the legal arguments complex. While we must be concerned with the efficiency of court proceedings, it is fundamental that efficiency not interfere with due process. While we have, we hope, rationalized the review procedure, we do not think that any genuine due process or privacy interests have been infringed. As is apparent, we have attempted to limit admissibility issues to substantive issues which go to the heart of the reasons for the controls.

Where the defence wishes to litigate all issues in a wiretap case, the evidence can include testimony as to installation of the device, monitoring the device, preparation of tapes and transcripts, continuity, voice identification, proof of designation of agents, and so on. Experience has shown that defence counsel will often waive proof of many of these matters when there is no useful purpose served in defence of their client. We have included certain recommendations in an attempt to streamline areas of inquiry and proof, which are usually noncontentious.

RECOMMENDATIONS

57. That the reasonable notice referred to in subsection 178.16(4) apply whenever the prosecution seeks to introduce an intercepted private communication.

58. That where the prosecution has failed to give reasonable notice, a justice presiding at a preliminary inquiry or the trial judge may adjourn the proceedings for the purpose of requiring the prosecution to give reasonable notice and take whatever other steps are required to ensure that reasonable notice is given prior to the proceedings, taking into consideration the right of the accused to a trial within a reasonable time.

59. That section 457.3 be amended by including paragraph (*d*.1) as follows:

the justice may receive evidence of an intercepted private communication or evidence obtained as a result of an interception of a private communication apparently made under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, section 178.16 does not apply to such evidence.

60. That primary evidence obtained by electronic surveillance be inadmissible unless:

(a) the interception was lawfully made

(i) with the consent of a party to the intercepted communication,

(ii) in accordance with the terms of an authorization;

(b) a party to the intercepted communication consents to the admission.

61. That where a defect exists on the face of the authorization or renewal, the trial judge shall admit the primary evidence obtained in apparent compliance with such authorization or renewal unless officers acting in apparent compliance therewith could not reasonably have believed that the authorization or renewal was valid.

62. That, for the purposes of Recommendation 51, a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed;

(b) reasonable and probable grounds to believe that a targeted offence was being committed by a person provided for in the authorization did not exist;

(c) any other grounds exist from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

63. That evidence which is derived from primary evidence which is inadmissible, is itself inadmissible where in the opinion of the court, having regard to all the circumstances, to admit such evidence would bring the administration of justice into disrepute.

64. That evidence is derived from primary evidence where it would not have been obtained but for the acquisition of the primary evidence. However, evidence is not derivative where:

(a) it is obtained pursuant to an otherwise valid authorization although such authorization was based on evidence obtained as a result of an invalid authorization;

(b) it is the testimony of a witness to the commission of an offence although the witness' identity was discovered as a result of inadmissible primary evidence.

65. That once primary evidence is determined to be inadmissible, Crown counsel shall stipulate what, if any, evidence is derivative therefrom and the reasons why any other evidence is not derivative. That for the purposes of determining the validity of such reasons, the prosecution or the accused may, with leave of the

court, call any witness for the purposes of cross-examination, and the accused with leave of the court may inspect any tapes or transcripts related to the investigation, whether or not he was a party to the communication.

66. That affidavit evidence be admissible and, in the absence of evidence to the contrary, be *prima facie* proof of:

(a) the times and places of the interception;

(b) the custody and continuity of the tape recordings;

(c) the manner of interception;

(d) service of notice.

67. That a copy of the authorization signed by a judge be admissible without proof of the authenticity of the signature.

68. That recital in the authorization as to the status of the designated agent be proof of such designation.

VI. Miscellaneous Recommendations

A. Annual Reports: Section 178.22

Section 178.22 of the *Criminal Code* requires the Solicitor General or provincial Attorney General to prepare essentially a statistical report. The Commission has previously studied the weakness of the section 178.22 report[266] and considered various recommendations designed to strengthen accountability in this area. We have also been told that the Department of Justice has certain recommendations which it wishes considered in this particular area. Unfortunately, their recommendations are not yet complete and it is difficult for us to assess the impact of our other recommendations designed to increase accountability.

While useful information can be obtained from review of statistics, we are hopeful that some of our recommendations concerning disclosure of material and notice will serve to make the entire process more open and accountable with a corresponding diminution in the need to rely on statistics. Accordingly, for the present, we have made no recommendation for amendments to section 178.22.

266. Savage, *supra*, note 44.

B. Notice under Section 178.23

The present legislation, section 178.23 of the *Criminal Code*, requires the minister on whose behalf the application for an authorization was made to give notice in writing to the person who was the object of the interception within a specified period. Thus, no notice is required to a person who was the object of a consent interception, that is, one not done by means of an authorization. It is the nature of a properly conducted interception, of course, that the persons targeted are never aware of the operation, particularly if charges are never laid. This illustrates the need for some form of post-interception notice.

Section 178.23 of the *Criminal Code* as presently interpreted requires that the person who was the object of the interception merely be told of that fact. As held in *Re Zaduk and The Queen*,[267] the person is entitled to no greater notification, such as the date or period of the interception, a copy of the authorization or access to the tape recordings. The American legislation requires a somewhat wider notice and gives a discretion to the court to give further discovery:

> S. 2518(8)
>
> (d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of —
>
> (i) the fact of the entry of the order or the application;
>
> (ii) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
>
> (iii) the fact that during the period wire or oral communications were or were not intercepted.
>
> The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.[268]

Since its enactment, virtually all persons who have considered the question have expressed dissatisfaction with the present notice procedure. It has been observed that in one sense the object of the interception would be better off not getting the notice, since the notice provided is so inadequate as to be useless and merely engenders anxiety and frustration. In our view, the notice under section 178.23 must be meaningful in relation to the purposes for which it is required. This calls for the identification of those purposes.

---

267. *Supra*, note 189.

268. Title III, *supra*, note 67, section 2518(8).

The case-law has identified two purposes. In *R.* v. ***Welsh and Iannuzzi (No. 6)***[269] and ***Re Zaduk and The Queen***, [270] the purpose identified was that of political accountability. In *Zaduk*, Mr. Justice Lacourcière described this accountability as flowing from the ability of the public "to monitor, in a general way, the application and practical effect of the new legislation." It was his view that section 178.23 was not intended as a means of advancing a civil suit for improper interception. As His Lordship pointed out, civil liability flows from "unlawful, i.e. unauthorized, interceptions." Weatherston J.A., dissenting, came to the opposite conclusion. It was his view that some mechanism must be available for furthering the civil remedies that could flow from an unlawful interception. As His Lordship pointed out, the authorization may have permitted some means of interception at certain places and not others. Without more information, the targeted person is left without any way of determining whether the interceptions actually conducted were within the terms of the authorization. To quote Justice Weatherston: "A citizen is entitled to the protection of the law. How can he enjoy that protection unless he knows the extent to which his rights have been invaded?"[271]

The problem of adequate civil remedies for unlawful interception is beyond the scope of this Paper. We have, therefore, not specifically approached this problem from the point of view of civil discovery. On the other hand, we feel that the principles of reviewability and accountability which have guided the work in the police powers areas call for more than section 178.23 now requires. An appropriate analogy is where the police search unoccupied premises under a warrant. In Working Paper 30[272] it is recommended that a copy of the warrant should be suitably affixed within any place that is unoccupied at the time of the search. It is an important principle that intrusions into privacy be justifiable and justified. At a minimum, therefore, the apparent justification for the massive intrusion by electronic surveillance must be given to the person affected. He should, therefore, be entitled to know when the intrusion took place and under what authority. We are also of the view that some mechanism should be in place for a further disclosure in an appropriate case. We consider these proposals to be the minimum where no charges are laid against the target and he does not have the fuller disclosure or notice mandated by section 178.16.

A recent decision of Steele J., styled *R.* v. *X*,[273] has pointed out a problem with the drafting of subsection 178.23(4). This provision gives a judge power to extend the period during which notification may be given by up to three years, provided *inter alia* "the investigation of the offence to which the authorization relates is continuing." It may happen, as in the *X* case, that the first authorization will be in relation to certain offences but that the investigation may have ceased. In the meantime, investigation into other offences for which new authorizations were obtained may be continuing. However, the wording of subsection 178.23(4) would preclude the judge from extending the notice

269. *Supra*, note 31.

270. *Supra*, note 189, p. 332.

271. *Id.*, p. 341.

272. *Supra*, note 47, Recommendation 27, p. 350.

273. *R.* v. *X*, Ont. H.C.J., *per* Steele J., May 15, 1984 (unreported).

period on the first authorization. In our view, the need for an extension is legitimate in the latter case, since any notification would likely frustrate the ongoing related investigation. Accordingly, the statute should be amended to cure this problem.

A further problem concerns sanctions for failure to give the section 178.23 notice. Case-law has uniformly held that failure to give notice has no effect on the admissibility of evidence where charges, in fact, are laid as a result of the investigation.[274]

Only in exceptional circumstances can exclusion of evidence be justified on the basis of noncompliance with statutory provisions that do not go to the legality of the interception. At present, the *Protection of Privacy Regulations*[275] require that the Attorney General or Solicitor General certify to the court the manner in which the notice was given. In the case where the person is never charged, so that the section 178.16 notice provisions never apply, this is adequate, subject to a slight change in wording to reflect that the certification requirement arises not simply "where the notice was given by him" but from the fact that notice is required under section 178.23. We see no need for any particular sanction in the absence of some particular indication that the present regime is not adequate.

Where charges are laid *and* notice is served under section 178.16, we think that such notice is adequate and see no requirement for further notice under section 178.23, having regard to the purposes for which the latter notice is given. However, where charges are laid and the Crown does not intend to rely on wiretap evidence, the accused may never get a notice under section 178.16 and never learn of the interception, unless there is compliance with section 178.23. Knowledge of the interception may be important to the accused's ability to make full answer and defence. In the recent case of *R.* v. *McLeod*,[276] one of the accused on a charge of murder relied on the defence of alibi. He was a member of a motorcycle gang, and unknown to him the gang's clubhouse was wiretapped. It was only after the conviction on appeal and by purely fortuitous circumstances that his counsel learned that tapes existed of his conversation the night of the killing, which tended to support the alibi. As a result, his conviction was set aside and a new trial ordered based on this fresh evidence.

Further, so long as there is even a limited exclusionary rule, it is important that the accused be aware of the existence of any interceptions. Some mechanism must be in place such as section 178.23 to provide him with that notice.

Finally, we have given some consideration to whether there should be notice in cases of consent interceptions. However, since the reason for post-interception notice really arises from the fact that none of the parties are aware of the interception, we do not believe the same policy considerations require notice in those cases. We would

274. *R.* v. *Welsh and Iannuzzi (No. 6)*, *supra*, note 31; *R.* v. *Miller and Thomas (No. 4)* (1975), 28 C.C.C. (2d) 128 (B.C. Co.Ct.).

275. *Protection of Privacy Regulations*, C.R.C. 1978, vol. 5, c. 440.

276. *R.* v. *McLeod*, Ont. C.A., April 13, 1982 (unreported).

also be concerned about possible danger to informers and other police operatives who, perhaps at some risk to themselves, had agreed to be bodypacked. On balance we see no need for notice outside the trial process in such circumstances.

After the project has concluded and the time comes to give notice, it may be that the person is no longer traceable. It is the policy of some police forces to serve the section 178.23 notice personally, even though the legislation does not require this, and to file an affidavit with the court when the party cannot be located. We feel that the affidavit procedure is a good one, although we consider that a signed statement by the officer is sufficient.

RECOMMENDATIONS

69. That where notice under subsection 178.16(4) has not been given, a person who was the object of an interception shall be given notice of the dates of the interceptions and a copy of the authorization under which the interception took place.

70. That, upon written application by the accused, a judge with power to grant an authorization, or the trial judge, may require the prosecution to disclose such details of interceptions as may be necessary for an accused to make full answer and defence.

71. That, for the purposes of Recommendation 65, the judge may require the prosecutor to make such inquiries of law enforcement agencies as the judge considers necessary.

72. That notice under section 178.23 shall be given within ninety days of the termination of the authorization or renewal or such greater period not exceeding three years, where a judge is satisfied that by reason of a continuing investigation the giving of notice within ninety days would be contrary to the interests of justice.

73. That where notice cannot be given under section 178.23 because the person cannot be located, a peace officer with knowledge of efforts made to locate the person shall submit a statement in writing to the court setting out the reasons why notice has not been given and efforts made to locate the person.

C. The Disclosure of Intercepted Private Communications

Section 178.2 of the *Criminal Code* enacts a prohibitory and preventive scheme which regulates the use and disclosure of intercepted private communications, in whole

or in part, or the substance, meaning, purport or existence of such whole or part, absent consent by a party to the interception, use or disclosure.[277]

The listed exceptions of subsection 178.2(2) exempt from the prohibition of the preceding subsection such use or disclosure as is made for investigative, evidentiary or service purposes. We see no reason to disagree with the rationale underlying such exemptions which represent, as we view it, a proper balance of privacy, law enforcement and fair trial considerations. There are, however, practical considerations which, consistent with the aforementioned *rationalia*, argue most persuasively in favour of at least a clarification if not expansion of the listed exceptions in subsection 178.2(2)

Investigations involving electronic surveillance characteristically produce hundreds if not thousands of hours of monitoring, corresponding transcripts of recorded communications, and seemingly endless interception logs. Significant evidentiary problems routinely emerge in such cases and, not infrequently, experienced prosecutorial assistance is sought to determine whether or what proceedings may be instituted. Indeed, independent prosecutorial review of the fruits of the interception process at such an early stage is highly desirable to ensure that only legally sufficient cases engage the attention of the criminal process. The present investigative disclosure exceptions, paragraphs 178.2(*b*) and (*e*), while arguably of sufficient breadth to permit the disclosure here considered, in our view, ought to be expanded so as to permit it expressly. The proposed expansion does not, in our view, compromise any recognizable privacy interest nor otherwise impair the spirit of the recommendations here made.

Private communications intercepted in accordance with an authorization granted by a competent Canadian judicial authority, on occasion, may afford evidence of crimes committed entirely beyond our borders or of offences about to take place there. There exists some divergence of opinion as to whether information obtained through judicially authorized Canadian interceptions can be lawfully transmitted to foreign law enforcement agencies. While it seems highly desirable that such information be made available to the appropriate authorities in foreign jurisdictions, if for no reason than to be consonant with some of our international obligations, it is of equivalent significance that such disclosure should only be to properly authorize investigative or law enforcement officers in limited circumstances. To put the matter somewhat differently, such disclosure ought to be permissible only when made to investigative or law enforcement officers in the foreign jurisdiction and to the extent that it reveals a past, current or potential crime in such jurisdiction.

RECOMMENDATION

74. That subsection 178.2(2) be amended expressly to exempt from the prohibition of subsection 178.2(1) the following:

(a) where the disclosure is made to a peace officer, the *Attorney General or his agent* and is intended to be in the interests of justice; and,

277. *Criminal Code*, s. 178.2(1).

(b) where the disclosure is made to an investigative or law enforcement officer in a foreign jurisdiction and tends to reveal a past, ongoing or prospective crime in such jurisdiction.

D. Assistance in the Execution of Orders

Intractable difficulties have arisen in the execution of judicial authorizations where assistance is required from persons in charge of premises in respect of which interceptions are to take place and organizations engaged in providing telephone, telegraph or other communications services. It has been found, for example, particularly in the provinces of Ontario and Québec, that interceptions authorized by judicial order cannot be carried out because the necessary information and assistance have not been furnished by the relevant communications company. The fact and extent of the invasion of privacy have been judicially determined, but the lack of assistance at least delays the execution of the order and, on occasion, entirely frustrates it.

Analogous arguments have earlier been rehearsed in connection with surreptitious entry. By parity of reasoning, we can see no justification for permitting explicit authority to be given to enter premises to install interception devices for the purpose of giving effect to an authorization, but withholding it where assistance falling short of an actual invasion of the target's property only is required. We would make two further observations. To include a statutory requirement of furnishing assistance as is done in section 2518(4) of Title III should also carry with it both an appropriate penalty for noncompliance and an exemption from interceptional liability under subsection 178.11(2). Secondly, the communication's organization ought to be compensated for its assistance at the prevailing rates for the service provided.

RECOMMENDATIONS

75. That the authorizing judge be given express authority to order any person, including companies and organizations, engaged in providing communication or telecommunication services, as well as landlords, custodians or persons in charge of premises, to furnish all such technical or material assistance or information as may reasonably be required to accomplish the interception in accordance with the authorization, and to be compensated therefor at the prevailing rates.

76. That failure of compliance in accordance with the authorization shall be punishable as contempt of court.[278]

278. See, for example, subsection 533(2) of the *Code*, which makes failure to comply with the terms of an order releasing exhibits for scientific or other testing or examination punishable as contempt.

CHAPTER FOUR

Summary of Recommendations

The Offence

1. That the offences for which an authorization would be available continue to be listed. That the following offences be omitted from the present list in section 178.1: *Criminal Code* ss. 58 (forgery, etc.), 159 (obscene material), 195(1)(*a*) (procuring), 281.1 (advocating genocide), 314 (theft from mail), 331 (threatening letters, etc.), 339 (using mails to defraud); and *Excise Act*: ss. 158 and 163 (unlawful distillation or selling of spirits).

2. That the following *Criminal Code* offences be added to the list: ss. 195(1)(*b*), (*c*), (*d*), (*h*) and (*i*) (procuring, etc.), 305.1 (criminal interest rate), 381.1 (threats to commit offences against internationally protected person).

3. That the organized crime definition for offences be omitted but an authorization be available for investigation of: a conspiracy to commit; attempt to commit; being an accessory after the fact; and counselling, procuring or inciting in relation to any of the listed offences.

Private Communications

4. That "private communications" be defined as follows:

> **any oral communication or any telecommunication made under circumstances in which it is reasonable for any party to it to expect that it will not be intercepted by any electromagnetic, acoustic, mechanical or other device.**

5. That a communication does not cease to be a private communication only by reason of a belief on the part of a party to it that the communication may be the subject of an authorization obtained from a court by a law enforcement agency.

6. That subsection 178.11(2) be amended by the addition of paragraph (*e*) as follows:

> **a person engaged in monitoring for security purposes of communications of inmates of a prison as defined by the *Prisons and Reformatories Act*, R.S.C. 1970, c. P-21, and a penitentiary as defined by the *Penitentiary Act*, R.S.C. 1970, c. P-6, where the fact that such monitoring may occur is prominently displayed at the place where the communication may occur.**

7. That the definition of "electromagnetic, acoustic, mechanical or other device" be amended as follows:

> **"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used, or is capable of being used, to intercept a private communication, but does not include a hearing-aid used to correct subnormal hearing of the user to not better than normal hearing, nor a device such as a pen register, touch-tone decoder, diode device or other similar device used to acquire the identity of the telephone number dialed, or of the caller, the time and the date of the telephone call, but which is not capable of intercepting any words or other information.**

Optical Devices

8. That it be an offence to enter private property without a court order or the consent of the owner or lawful occupier for the purpose of installing an optical device.

9. That an authorization to install an optical device be available by application to a court, but only under the same conditions as an authorization is available for installation, by surreptitious entry, of a listening device.

10. That "optical device" be defined for the present time as any electronic device or mechanism capable of permitting surreptitious viewing of persons or things.

Foreign Interceptions

11. That primary and derivative evidence obtained from an interception made outside Canada, no matter where the private communication originated, be admissible in evidence whether or not the interception was lawfully made, provided that the interception was not made in the foreign jurisdiction in violation of the laws of the jurisdiction with the connivance of Canadian authorities.

12. That the court before which evidence from a foreign interception is tendered shall conduct an inquiry into the admissibility of that evidence only where

the person against whom the evidence is sought to be admitted leads some evidence from which the court could find that the interception was made in violation of the laws of the foreign jurisdiction with the connivance of Canadian authorities.

13. That the notice provisions in present *Code* subsection 178.16(4) apply to evidence obtained from foreign interceptions.

Participant Monitoring: Consent Interceptions

14. That section 178.11 continue to provide that it is not unlawful to intercept private communications where the interception is made with the consent, express or implied, of any party to it.

15. That the offence in subsection 178.18(1) not apply to any person in possession of a device or component for the purpose of using it in an interception made or to be made with the consent of one of the parties.

16. (1) That a peace officer, before commencing an interception under this section, shall inform the person whose consent is sought that he has a right to refuse to consent and to withdraw his consent at any time.

(2) That consent under this section may be given orally or in writing.

17. That the signature of a person on a document warning him of his right to refuse to consent and of his right to withdraw his consent at any time or a recording of such consent be *prima facie* proof of the consent of the person to the interception.

The Application Procedure

18. That the application for an authorization or renewal continue to be in writing and accompanied by an affidavit of a peace officer. The hearing shall be *ex parte* and *in camera*. The judge should be empowered to place the peace officer under oath to ascertain additional facts underlying the application. However, if such facts are relied upon in the adjudication of the application, a record of such facts shall be included in the sealed packet.

Basis for Granting the Authorization

19. That paragraph 178.13(1)(*a*) be amended to provide that the judge may grant an authorization where he is satisfied that it would be in the best interest of the administration of justice and in the public interest having regard to the seriousness of the offence under investigation.

Interprovincial Offences

20. That subsection 178.12(1) be amended to provide that an authorization may be granted where the communications of the targeted person may be intercepted in one province, although the offence is alleged to have been committed in another province.

Minimization

21. That an authorization may only be granted in relation to persons the interception of whose private communications will assist in the investigation of the offence by reason of their involvement in the offence.

22. That section 178.13 be amended to provide that the judge, in granting the application, may include any of the following terms and conditions:

(a) that the device be live monitored at all times that it is proposed to intercept or record private communications;

(b) that o far as is reasonably possible, only the conversations of targeted persons be intercepted and recorded;

(c) that where it is proposed to intercept communications at a telephone to which the public has a right of access, then any interceptions shall be on the basis of live monitoring and accompanied by visual surveillance;

(d) that reasonable steps be taken not to intercept private communications between spouses, physician and patient or persons in other confidential relationships;

(e) that reasonable steps be taken not to intercept private communications of targeted persons which by reason of a known pattern are unlikely to assist in the investigation of the offence;

(f) that interception cease after the object of the investigation has been obtained;

(g) that, where the interception of a telephone line will involve a party line, no interception occur except when the line is being monitored;

(h) such further terms and conditions as the judge considers advisable to minimize the acquiring and recording of private communications which would not assist in the investigation.

23. That the authorization shall include a term requiring that, where an interception is to occur at a place mentioned in subsection 178.13(1.1), reasonable steps shall be taken to ensure that privileged communications between solicitors and clients are neither intercepted nor recorded.

24. That where there are grounds to suspect that if an authorization is granted, privileged communications between the targeted person and his solicitor will be intercepted, that fact shall be disclosed in the application to obtain an authorization.

25. That in a case to which Recommendation 21 applies, the authorization shall include a term that, so far as reasonably possible, privileged communications between the targeted person and his counsel not be intercepted or recorded.

Basket Clauses

26. That subject to Recommendation 27, the authorization shall contain a clause naming or otherwise identifying the persons the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

27. That, in addition, the authorization may contain a clause permitting the interception of a class of unidentified persons whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

28. That subject to Recommendation 29, the authorization shall limit the interceptions to specified premises.

29. That the authorization may contain a clause permitting interception of private communications at other than specified premises where the other place is resorted to by persons known and identified in the authorization. At such premises, only those communications to which the known and identified person is a party may be intercepted, unless the specially designated agent has applied in writing to the authorizing judge as soon as practicable for amendment of the authorization. The application for an amendment shall be supported by the affidavit of a peace officer setting out the reasons for interception at these premises, the names of the persons whose communications are likely to be intercepted and the reasons why interception at such premises is required. The judge may refuse to amend the order, or amend the order, which amendment is effective from the date when interception commenced at the additional premises, unless the judge is not satisfied that the application was made as soon as practicable, in which case the amendment may be made effective at such later date as the judge sees fit in the circumstances.

30. That the legislation contain a list of terms or conditions which *may* be included in the authorization, such as the following:

(a) that periodic reports be made to the authorizing judge as to the identities of persons whose communications are being intercepted pursuant to a basket clause;

(b) that periodic reports be made to the authorizing judge as to the places, not specifically named in the authorization, where interceptions are taking place.

Surreptitious Entry

31. That the authorizing judge be given power to authorize an entry onto private premises without the consent of the occupier, for the installation, removal or servicing of an electromagnetic, acoustic, mechanical or other device.

32. That the authorizing judge may only so authorize where the circumstances of the offence are serious and there is a high degree of likelihood that relevant evidence will be obtained.

33. That an application for an authorization which includes an authorization to make a surreptitious entry shall state the reasons why such entry is required and why other less intrusive means will not be sufficient.

34. That it be an offence to enter private premises without the consent of the occupier for the purpose of installing, servicing or removing an electromagnetic, acoustic, mechanical or other device without an order under Part IV.1 of the *Criminal Code*, and an offence to remove anything from the premises at the time of the entry.

35. That the peace officer making the entry should not be entitled to use force against any person for the purpose of effecting such entry or exit, except as necessary to protect himself or others.

36. That the authorizing judge may order that certain means be used/not used to effect the entry.

37. That following the investigation, the owner and occupier of the premises be notified of the entry and be given a copy of the order which authorized the entry.

38. That reasonable steps be taken to repair any damage to the premises or to compensate the owner for any significant damage left unrepaired.

39. That the use of a small amount of electricity to enable the device to function shall not constitute a criminal offence.

Renewals

40. That where, to the knowledge of the designated agent or the deponent of the affidavit made in support of an authorization, an authorization has previously been granted in relation to the same or a related investigation, the application shall contain the information referred to in paragraph 178.13(3)(*b*) of the *Code*.

41. That a renewal of an authorization may include the names of persons previously provided for in the authorization but unnamed in the authorization.

42. That a renewal of an authorization may include additional places of interception of persons provided for in the original authorization.

43. That minor variations of the terms of the authorization may be included in a renewal, including the following:

(a) different or more accurate descriptions of persons or places;

(b) different or additional means of interception;

(c) different or additional offences clearly related to the offences in the original authorization and part of the same investigation.

44. That a renewal of an authorization may include terms not included in the original authorization, designed to minimize interceptions of communications which are not related to the offence.

45. That a renewal shall be for a period not exceeding thirty days, with the exception that where special cause is shown, a renewal may be for a period not exceeding sixty days. "Special cause" in this recommendation means circumstances making it probable that the investigation will not be completed within thirty days *and* it would be impracticable to obtain a further renewal within thirty days. Where the period of a renewal exceeds thirty days, the judge shall indicate on the face of the authorization the reasons therefor, with reference to the particular circumstances of the investigation.

46. That in any case referred to in Recommendation 45, the judge shall ensure that a renewal would not be available in the circumstances. In no case shall an authorization be granted where there is reason to suspect that it is intended to avoid the effect of Recommendation 45. Where the only reason that a renewal is unavailable is because the previous renewal or authorization has expired, then the subsequent authorization shall be for thirty days, unless special cause has been shown.

47. That the legislation provide for a list of terms and conditions which may be included in the renewal such as the following:

(a) that the interception shall terminate once the objective of the original authorization is achieved;

(b) that any applications for subsequent renewals or authorizations be made to the judge who granted the original authorization or renewal.

48. That section 178.14 of the *Criminal Code* be amended to include the following:

(a) in addition to the exceptions provided for in present paragraph (1)(*a*), to allow access to the material in the sealed packet for the purpose of dealing with an application for an authorization in related investigations;

(b) to permit the specially designated agent to retain a true copy of all the documents relating to an application made pursuant to section 178.12 or subsection 178.13(3).

49. That the prosecutor, when giving notice under subsection 178.16(4), shall include: a copy of the authorization and renewals under which the interceptions were made; and, subject to the order of a court, a copy of all the documents relating to an application for the authorization or renewal.

50. That prior to giving notice pursuant to subsection 178.16(4), the specially designated agent may apply to a judge as defined in section 482 of the *Criminal Code ex parte* and *in camera* for an order that certain portions of the material not be disclosed on the basis that disclosure could tend to reveal the identity of an informer or of any other person who has assisted with the investigation and in the latter case it is shown that it would not be contrary to the public interest that the identity of such persons be withheld. The application should be in writing and supported by the affidavit of a peace officer.

51. That the person against whom evidence is sought to be admitted pursuant to paragraph 178.16(1)(*a*) of the *Criminal Code* by reason of an interception made pursuant to an authorization or renewal, may apply at the preliminary inquiry or the trial to exclude that evidence and derivative evidence on the basis of a substantive defect in the application for the authorization or renewal. The following procedure would apply:

(a) The application should be in writing and supported by affidavit evidence (or *viva voce* evidence with leave of the judge).

(b) Only if the application and the evidence in support when considered together with the material disclosed under Recommendation 49 raises a real question as to whether there is a substantive defect in the application as defined in Recommendation 62 which could lead to the exclusion of evidence, shall the judge hold an inquiry as to the validity of the application for the authorization or renewal.

(c) Should the judge direct an inquiry, the burden of proof is on the Crown to satisfy the court that there was no substantive defect in the application as defined in Recommendation 62.

(d) The affidavit and testimony of the accused is not admissible at the instance of the Crown at the preliminary hearing or trial.

Emergency Authorization: Section 178.15

52. That section 178.15 be amended by the addition of subsection (6) as follows:

The admissibility of evidence acquired as a result of an order obtained under this section is not affected by the fact that the electromagnetic, acoustic, mechanical or other device was installed prior to the obtaining of the order, where the order under this section was obtained in relation to the offence under subsection 247(1) (kidnapping) and no private communications were acquired through use of the device until the order was obtained.

53. That an application for an emergency authorization under section 178.15 shall be made in writing or by telephone or other means of telecommunication and there shall be a record including: a statement of the reasons why an authorization could not, with reasonable diligence, be obtained under section 178.13; the facts relied upon to justify the belief that an authorization should be given, together with particulars of the offence; the persons whose private communications it is sought to intercept; and, the places of interception.

Admissibility of Evidence of Other Offences

54. That where the prosecution seeks to adduce primary evidence obtained by means of an authorization at the preliminary inquiry or trial of offences none of which are named in the authorization, the judge shall conduct a *voir dire* for the purpose of determining whether the interception of evidence of such offences was done in good faith.

55. That for the purposes of Recommendation 54, "good faith" means:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception;

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of

such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because

(i) the grounds for suspicions were not strong enough to meet the statutory test,

(ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

56. That where he is not satisfied that the interception of other offences was done in good faith, the judge shall exclude primary evidence and may exclude evidence shown to be derivative, where he is satisfied that to permit such evidence to be adduced would bring the administration of justice into disrepute.

Remedies: Admissibility of Evidence

57. That the reasonable notice referred to in subsection 178.16(4) apply whenever the prosecution seeks to introduce an intercepted private communication.

58. That where the prosecution has failed to give reasonable notice, a justice presiding at a preliminary inquiry or the trial judge may adjourn the proceedings for the purpose of requiring the prosecution to give reasonable notice and take whatever other steps are required to ensure that reasonable notice is given prior to the proceedings, taking into consideration the right of the accused to a trial within a reasonable time.

59. That section 457.3 be amended by including paragraph (*d*.1) as follows:

the justice may receive evidence of an intercepted private communication or evidence obtained as a result of an interception of a private communication apparently made under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, section 178.16 does not apply to such evidence.

60. That primary evidence obtained by electronic surveillance be inadmissible unless:

(a) the interception was lawfully made

(i) with the consent of a party to the intercepted communication,

(ii) in accordance with the terms of an authorization;

(b) a party to the intercepted communication consents to the admission.

61. That where a defect exists on the face of the authorization or renewal, the trial judge shall admit the primary evidence obtained in apparent compliance with such authorization or renewal unless officers acting in apparent compliance therewith could not reasonably have believed that the authorization or renewal was valid.

62. That, for the purposes of Recommendation 51, a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed;

(b) reasonable and probable grounds to believe that a targeted offence was being committed by a person provided for in the authorization did not exist;

(c) any other grounds exist from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

63. That evidence which is derived from primary evidence which is inadmissible, is itself inadmissible where in the opinion of the court, having regard to all the circumstances, to admit such evidence would bring the administration of justice into disrepute.

64. That evidence is derived from primary evidence where it would not have been obtained but for the acquisition of the primary evidence. However, evidence is not derivative where:

(a) it is obtained pursuant to an otherwise valid authorization although such authorization was based on evidence obtained as a result of an invalid authorization;

(b) it is the testimony of a witness to the commission of an offence although the witness' identity was discovered as a result of inadmissible primary evidence.

65. That once primary evidence is determined to be inadmissible, Crown counsel shall stipulate what, if any, evidence is derivative therefrom and the reasons why any other evidence is not derivative. That for the purposes of determining the validity of such reasons, the prosecution or the accused may, with leave of the court, call any witness for the purposes of cross-examination, and the accused with leave of the court may inspect any tapes or transcripts related to the investigation, whether or not he was a party to the communication.

66. That affidavit evidence be admissible and, in the absence of evidence to the contrary, be *prima facie* proof of:

(a) the times and places of the interception;

(b) the custody and continuity of the tape recordings;

(c) the manner of interception;

(d) service of notice.

67. That a copy of the authorization signed by a judge be admissible without proof of the authenticity of the signature.

68. That recital in the authorization as to the status of the designated agent be proof of such designation.

Notice under Section 178.23

69. That where notice under subsection 178.16(4) has not been given, a person who was the object of an interception shall be given notice of the dates of the interceptions and a copy of the authorization under which the interception took place.

70. That, upon written application by the accused, a judge with power to grant an authorization, or the trial judge, may require the prosecution to disclose such details of interceptions as may be necessary for an accused to make full answer and defence.

71. That, for the purposes of Recommendation 65, the judge may require the prosecutor to make such inquiries of law enforcement agencies as the judge considers necessary.

72. That notice under section 178.23 shall be given within ninety days of the termination of the authorization or renewal or such greater period not exceeding three years, where a judge is satisfied that by reason of a continuing investigation the giving of notice within ninety days would be contrary to the interests of justice.

73. That where notice cannot be given under section 178.23 because the person cannot be located, a peace officer with knowledge of efforts made to locate the person shall submit a statement in writing to the court setting out the reasons why notice has not been given and efforts made to locate the person.

The Disclosure of Intercepted Private Communications

74. That subsection 178.2(2) be amended expressly to exempt from the prohibition of subsection 178.2(1) the following:

(a) where the disclosure is made to a peace officer, the *Attorney General or his agent* and is intended to be in the interests of justice; and,

(b) where the disclosure is made to an investigative or law enforcement officer in a foreign jurisdiction and tends to reveal a past, ongoing or prospective crime in such jurisdiction.

75. That the authorizing judge be given express authority to order any person, including companies and organizations, engaged in providing communication or telecommunication services, as well as landlords, custodians or persons in charge of premises, to furnish all such technical or material assistance or information as may reasonably be required to accomplish the interception in accordance with the authorization, and to be compensated therefor at the prevailing rates.

76. That failure of compliance in accordance with the authorization shall be punishable as contempt of court.

Rapports et documents de travail de la Commission de réforme du droit du Canada

Rapports au Parlement

1. *La preuve* (19 déc. 1975)
2. *Principes directeurs — Sentences et mesures non sentencielles dans le processus pénal** (6 fév. 1976)
3. *Notre droit pénal* (25 mars 1976)
4. *L'expropriation** (8 avril 1976)
5. *Le désordre mental dans le processus pénal** (13 avril 1976)
6. *Le droit de la famille** (4 mai 1976)
7. *L'observance du dimanche** (19 mai 1976)
8. *La saisie des rémunérations versées par la Couronne du chef du Canada** (19 déc. 1977)
9. *Procédure pénale — Première partie : amendements divers** (23 fév. 1978)
10. *Les infractions sexuelles** (29 nov. 1978)
11. *Le chèque** (8 mars 1979)
12. *Le vol et la fraude** (16 mars 1979)
13. *Les commissions consultatives et les commissions d'enquête* (18 avril 1980)
14. *Le contrôle judiciaire et la Cour fédérale** (25 avril 1980)
15. *Les critères de détermination de la mort* (8 avril 1981)
16. *Le jury* (28 juill. 1982)
17. *L'outrage au tribunal** (18 août 1982)
18. *L'obtention de motifs avant la formation d'un recours judiciaire — Commission d'appel de l'immigration* (16 déc. 1982)
19. *Le mandat de main-forte et le télémandat* (22 juill. 1983)
20. *Euthanasie, aide au suicide et interruption de traitement* (11 oct. 1983)
21. *Les méthodes d'investigation scientifiques : l'alcool, la drogue et la conduite des véhicules* (10 nov. 1983)
22. *La communication de la preuve par la poursuite* (15 juin 1984)
23. *L'interrogatoire des suspects* (19 nov. 1984)
24. *Les fouilles, les perquisitions et les saisies* (22 mars 1985)
25. *Les techniques d'investigation policière et les droits de la personne* (12 juin 1985)
26. ***Les organismes administratifs autonomes — Un cadre pour la prise de décisions*** (23 oct. 1985)

Documents de travail

1. *Le tribunal de la famille** (1974)
2. *La notion de blâme — La responsabilité stricte** (1974)
3. *Les principes de la détermination de la peine et du prononcé de la sentence** (1974)
4. *La communication de la preuve** (1974)
5. *Le dédommagement et l'indemnisation** (1974)
6. *L'amende** (1974)
7. *La déjudiciarisation** (1975)
8. *Les biens des époux** (1975)
9. *Expropriation** (1975)
10. *Les confins du droit pénal : leur détermination à partir de l'obscénité** (1975)
11. *Emprisonnement — Libération** (1975)
12. *Les divorcés et leur soutien** (1975)
13. *Le divorce** (1975)
14. *Processus pénal et désordre mental** (1975)
15. *Les poursuites pénales : responsabilité politique ou judiciaire** (1975)
16. *Responsabilité pénale et conduite collective** (1976)
17. *Les commissions d'enquête — Une nouvelle loi** (1977)
18. *La Cour fédérale — Contrôle judiciaire** (1977)
19. *Le vol et la fraude — Les infractions* (1977)
20. *L'outrage au tribunal — Infractions contre l'administration de la justice** (1977)
21. *Les paiements par virement de crédit* (1978)
22. *Infractions sexuelles** (1978)
23. *Les critères de détermination de la mort** (1979)
24. *La sterilisation et les personnes souffrant de handicaps mentaux* (1979)
25. *Les organismes administratifs autonomes* (1980)
26. *Le traitement médical et le droit criminel* (1980)
27. *Le jury en droit pénal** (1980)
28. *Euthanasie, aide au suicide et interruption de traitement* (1982)
29. *Partie générale : responsabilité et moyens de défense* (1982)
30. *Les pouvoirs de la police : les fouilles, les perquisitions et les saisies en droit pénal** (1983)
31. *Les dommages aux biens — Le vandalisme* (1984)
32. *L'interrogatoire des suspects* (1984)
33. *L'homicide* (1984)
34. *Les méthodes d'investigation scientifiques* (1984)
35. *Le libelle diffamatoire* (1984)
36. *Les dommages aux biens — Le crime d'incendie* (1984)
37. *La juridiction extra-territoriale* (1984)
38. *Les voies de fait* (1985)
39. *Les procédures postérieures à la saisie* (1985)
40. *Le statut juridique de l'Administration fédérale* (1985)
41. *L'arrestation* (1985)
42. *La bigamie* (1985)
43. *Les techniques de modification du comportement et le droit pénal* (1985)
44. *Les crimes contre l'environnement* (1985)
45. *La responsabilité secondaire* (1985)
46. *L'omission, la négligence et la mise en danger* (1985)

La Commission a également publié au-delà de soixante-dix documents d'étude portant sur divers aspects du droit. Pour obtenir le catalogue des publications, écrire à : Commission de réforme du droit du Canada, 130 rue Albert, Ottawa (Ontario) K1A 0L6, ou Bureau 310, Place du Canada, Montréal (Québec) H3B 2N2.

---

* Ces documents sont épuisés mais ils peuvent être consultés dans de nombreuses bibliothèques.

LA SURVEILLANCE ÉLECTRONIQUE

On peut obtenir ce document gratuitement en écrivant à :

Commission de réforme du droit du Canada
130, rue Albert, 7e étage
Ottawa, Canada
K1A 0L6

ou

Bureau 310
Place du Canada
Montréal (Québec)
H3B 2N2

© Commission de réforme du droit du Canada 1986
N° de catalogue J32-1/47-1986
ISBN 0-662-53886-2

Commission de réforme
du droit du Canada

Document de travail 47

LA SURVEILLANCE ÉLECTRONIQUE

1986

La Commission

M. le juge Allen M. Linden, président
M^e^ Gilles Létourneau, vice-président*
M^e^ Louise Lemelin, c.r., commissaire
M^e^ Joseph Maingot, c.r., commissaire
M^e^ John Frecker, commissaire*

Secrétaire par intérim

Harold J. Levy, LL.B., LL.M.

Coordonnateur de la section de recherche en procédure pénale

Stanley A. Cohen, B.A., LL.B.

Conseillers

Marc Rosenberg, B.A., LL.B.
David Watt, c.r., B.A., LL.B.

* N'était pas membre de la Commission lorsque le présent document a été approuvé.

Avis

Ce document de travail présente l'opinion de la Commission à l'heure actuelle. Son opinion définitive sera exprimée dans le rapport qu'elle présentera au ministre de la Justice et au Parlement, après avoir pris connaissance des commentaires faits dans l'intervalle par le public.

Par conséquent, la Commission serait heureuse de recevoir tout commentaire à l'adresse suivante :

Secrétaire
Commission de réforme du droit du Canada
130, rue Albert
Ottawa, Canada
K1A 0L6

Table des matières

CHAPITRE UN : Historique 1

I. Le point de vue du common law 1

II. Le comité Ouimet 2

III. La législation fédérale en matière de protection de la vie privée 3

A. Le projet de loi C-176 3

B. Le projet de loi C-51 5

CHAPITRE DEUX : Arguments en faveur d'une réforme 7

I. Introduction 7

II. Le cadre constitutionnel 8

III. L'équilibre entre le respect de la vie privée et l'application efficace de la loi 10

IV. Le rôle des juges 12

CHAPITRE TROIS : Recommandations et commentaires 15

I. L'application de la Partie IV.1 du *Code criminel* 15

A. L'infraction 15

B. Les communications privées 19

C. Les dispositifs optiques 24

D. L'interception de communications privées à l'étranger 26

E. La surveillance participative : l'interception consensuelle 30

II. L'autorisation 34
A. La demande d'autorisation 34
B. Les motifs de l'autorisation 35
C. Les infractions interprovinciales 36
D. La restriction des interceptions 38
E. Les clauses générales 44
F. L'entrée clandestine 48
G. Les renouvellements 56

III. La vérification de l'autorisation et le secret 59
A. Introduction 59
B. La vérification de l'autorisation 60
C. Le secret 67
D. Conclusion 70
(1) Premier point : À quel moment la question est-elle étudiée? 71
(2) Deuxième point : Comment la question est-elle résolue? 72

IV. L'autorisation en cas d'urgence : l'article 178.15 74

V. Les recours 75
A. La recevabilité de la preuve relative à d'autres infractions 75
B. Le recours en cas de dérogation au régime législatif 78
(1) Introduction 78
(2) La question de l'exclusion en général 79
C. Le préavis en vertu du paragraphe 178.16(4) 82
D. Le vice de fond dans la demande 83
(1) Le recours en droit délictuel 89
(2) La responsabilité pénale 90
(3) Le contrôle extrajudiciaire 90
(4) La règle d'exclusion 91
E. La preuve dérivée 95
F. La longueur des procédures 97

VI. Recommandations diverses 100

A. Les rapports annuels : l'article 178.22 100

B. L'avis en vertu de l'article 178.23 101

C. La divulgation des communications privées interceptées 105

D. L'aide dans l'exécution des ordonnances 106

CHAPITRE QUATRE : Sommaire des recommandations 109

CHAPITRE UN

Historique

I. Le point de vue du common law

Le common law ne range pas l'intimité de la vie privée au nombre des droits distincts devant faire l'objet d'une protection juridique spécifique. Ni l'avènement de la technologie électronique moderne, ni la prolifération subséquente des dispositifs de surveillance n'ont changé cet état de choses. Bien que certains recours civils[1] et poursuites pénales[2] puissent assurer, de façon incidente, une certaine protection du droit à la vie privée, ces mesures visent surtout d'autres droits garantis par la loi[3]. Elles ont d'ailleurs été jugées inefficaces à plusieurs égards. En premier lieu, elles ne pouvaient réparer le préjudice subi puisque l'ingérence dans la vie privée consiste à s'immixer dans les pensées, les émotions et les sensibilités de la personne. Ces mesures mettaient plutôt l'accent sur [TRADUCTION] «la nécessité de prouver d'abord qu'un préjudice réel, autre que l'insulte ou la peine ressentie», avait été causé, ce qui rendait [TRADUCTION] «la plupart des vieilles actions prévues par le common law inefficaces à préserver l'intimité de la personne, objet de la protection du droit au respect de la vie privée[4]». En deuxième lieu, les recours du droit pénal, les poursuites pour infraction au *Code criminel*, étaient également inutiles. Ces remèdes ne visaient ni la reconnaissance ni la protection du droit à la vie privée car ils avaient surtout été conçus en fonction d'autres droits garantis par le droit pénal[5]. En troisième lieu, ces remèdes étaient anachroniques, tant en matière civile que pénale, compte tenu du développement des technologies modernes grâce auxquelles une intrusion peut être commise sans l'être réellement et, à plus forte raison, sans qu'une infraction pénale ne soit perpétrée au sens ordinaire du terme[6].

1. Par exemple, une action en responsabilité pour entrée non autorisée, trouble de voisinage ou atteinte à la personne du demandeur ou à ses biens mobiliers ou immobiliers.
2. Voir, par exemple, *R.* v. *Chapman and Grange*, [1973] 2 O.R. 290, 11 C.C.C. (2d) 84 (C.A.). Il se peut que la conduite de D ait été également visée par les alinéas 381(1)*c*) ou *f*) du *Code criminel*, S.R.C. 1970, chap. C-34.
3. Par exemple, les atteintes à la jouissance d'un immeuble sanctionnées par une action en responsabilité pour entrée non autorisée ou troubles de voisinage.
4. Law Reform Commission of Australia, *Privacy and Intrusions* [Discussion Paper No. 13], juin 1980, p. 24-25.
5. Par exemple, l'intégrité des rapports contractuels et commerciaux visés par la Partie VIII du *Code criminel*, ou les droits de propriété protégés par les Parties VII et IX.
6. Comité de la réforme pénale et correctionnelle, *Rapport — Justice pénale et correction : un lien à forger*, Ottawa, Information Canada, 1969, p. 87 (ci-après appelé le rapport Ouimet).

Ajoutons enfin, qu'en common law, les règles de la preuve portent principalement sur la pertinence des éléments de preuve et non sur leur mode d'obtention. Les éléments de preuve pertinents sont recevables indépendamment de leur mode d'obtention[7], pourvu, bien sûr, qu'ils ne soient pas exclus par une règle du droit de la preuve. Somme toute, le pouvoir discrétionnaire d'écarter un élément de preuve, qui serait autrement recevable, demeure très limité[8]. Les éléments de preuve obtenus par suite d'une intrusion dans la vie privée, par exemple par l'enregistrement clandestin de communications téléphoniques, sont recevables en common law, en dépit de l'illégalité du procédé utilisé pour les obtenir, s'ils sont pertinents et que leur authenticité est convenablement attestée[9].

II. Le comité Ouimet

Dans son rapport publié en 1969, le comité Ouimet[10] était d'avis que le législateur fédéral devait protéger le secret des conversations qui se tiennent dans des conditions qui donnent aux *deux* interlocuteurs tout lieu de croire que leurs propos ne sont pas captés par des tiers, à l'aide de dispositifs électroniques, mécaniques ou autres[11]. À titre d'exception, l'interception de conversations privées en vue de faire respecter la loi et dans des conditions de contrôle rigoureux devrait être autorisée[12]. Selon le Comité, l'interception de conversations avec le consentement de l'un des interlocuteurs (surveillance participative), l'écoute à l'aide de postes téléphoniques supplémentaires et l'interception de conversations ayant lieu dans des conditions qui ne permettent pas à ceux qui y prennent part de s'attendre à ce qu'elles restent secrètes, ne réclament pas de contrôle législatif[13].

Le Comité préconisait l'adoption d'un système de contrôle judiciaire pour autoriser le branchement clandestin de lignes téléphoniques ou l'écoute clandestine à l'aide d'appareils électroniques et il a proposé un régime à cet effet[14].

La question de la recevabilité des conversations recueillies grâce à l'écoute clandestine et à la surveillance électronique a été examinée. Le Comité, qui avait proposé de ne pas adopter une règle stricte écartant toutes les autres preuves obtenues illégalement et de plutôt prévoir un pouvoir discrétionnaire de rejeter ces preuves, a suggéré

7. *Kuruma* v. *The Queen*, [1955] A.C. 197 (P.C.).
8. *R.* c. *Wray*, [1971] R.C.S. 272, [1970] 4 C.C.C. 1.
9. La jurisprudence antérieure portait principalement sur la pertinence de la preuve de telles questions.
10. *Supra*, note 6.
11. *Id.*, p. 88-89.
12. *Id.*, p. 90.
13. *Id.*, p. 92.
14. *Id.*, p. 93.

une règle distincte en vertu de laquelle les conversations interceptées illégalement seraient irrecevables parce qu'il est difficile de prétendre que ces preuves ont été recueillies par erreur ou inadvertance[15].

En résumé, comme le comité Ouimet avait conclu à la nécessité d'élaborer des dispositions pénales pour réprimer l'usage de l'écoute clandestine et la surveillance électronique à des fins criminelles, les éléments de preuve obtenus grâce à de tels procédés devaient aussi être écartés. Du même coup, le Comité reconnaissait que la mise en œuvre efficace de la loi exigeait le recours à la surveillance électronique comme méthode d'investigation. Tout en étant disposé à faire une exception, le Comité a clairement indiqué que le recours à de tels procédés devrait être assujetti à une autorisation judiciaire et faire l'objet d'une surveillance stricte[16].

III. La législation fédérale en matière de protection de la vie privée

La nécessité d'adopter une loi fédérale pour régir le recours à l'écoute clandestine et à la surveillance électronique, qu'avait soulignée le comité Ouimet en 1969, a été reconnue concrètement le 30 juin 1974 par la proclamation de la *Loi sur la protection de la vie privée*[17].

A. Le projet de loi C-176

Le 13 avril 1973, le ministre de la Justice a déposé devant la Chambre des communes le projet de loi C-176. Le caractère envahissant de la surveillance électronique autorisée est maintenu dans le projet de loi C-176 qui reprend la définition donnée au mot infraction dans le projet de loi C-252, à savoir :

> « infraction» désigne une infraction établie par une loi du Parlement du Canada et pour laquelle un contrevenant peut être poursuivi par voie de mise en accusation et comprend toute infraction de ce genre dont on allègue ou soupçonne la commission ou dont on croit la commission possible en se fondant sur des motifs raisonnables.

De même, les projets de loi conservaient la distinction entre les principes applicables à la recevabilité de la preuve primaire et ceux qui déterminent l'admissibilité de la preuve dérivée. Dans le premier cas, l'irrecevabilité était la règle, la recevabilité l'exception. Dans le cas de la preuve dérivée, il semble que ce soit le contraire[18].

---

15. *Id.*, p. 94-95.

16. Il a été notamment proposé que les rubans sur lesquels des conversations avaient été enregistrées conformément à l'ordonnance soient retournés au juge qui avait accordé l'autorisation.

17. S.C. 1973-1974, chap. 50.

18. La preuve dérivée n'a pas été jugée irrecevable uniquement parce que la preuve primaire dont elle découlait avait elle-même été exclue.

Le projet de loi C-176 a été examiné en détail publiquement. De nombreuses modifications ont été proposées, bien que la grande majorité ait été rejetée[19]. Seules trois d'entre elles méritent que nous nous y attardions.

À la première lecture du projet de loi C-176, le mot «infraction», défini à l'article 178.1, visait autant les manquements à toute loi fédérale pour lesquels leur auteur pouvait être poursuivi par voie de mise en accusation[20] que les infractions présumées à ces lois ou celles que l'on croyait, pour des motifs raisonnables, susceptibles d'être commises. Après une première modification, la définition comportait une liste d'infractions, jugées suffisamment graves en elles-mêmes, qui se prêtaient particulièrement bien à l'usage de la surveillance électronique ou caractérisaient l'activité du crime organisé. Outre les incriminations spécifiques, cette disposition visait les complots, les tentatives et la complicité après le fait à l'égard de ces infractions. Une périphrase constituait le dernier élément de la définition qui visait les activités du «crime organisé»[21]. On estimait que le champ d'application plus limité de la définition modifiée et adoptée par la Chambre des communes, atténuerait le caractère envahissant de cette méthode d'investigation.

Par suite d'une deuxième modification, la Chambre des communes remplaçait la disposition relative à la demande d'autorisation en cas d'urgence, qui avait été proposée antérieurement, par un nouvel article 178.15. Initialement, la participation d'un fonctionnaire judiciaire n'était pas prévue, sauf de façon rétroactive. La délivrance des autorisations dans les cas urgents relevait du procureur général d'une province, du solliciteur général du Canada ou de leurs mandataires respectifs spécialement désignés par écrit à cette fin. L'adoption de ces modifications par la Chambre des communes rendait nécessaire l'autorisation judiciaire et consacrait l'actuel régime.

La dernière modification apportée par la Chambre des communes concerne la recevabilité de la preuve primaire et de la preuve dérivée. L'adoption du paragraphe 178.16(3) permettait l'admission de preuves primaires et dérivées en dépit de vices de forme ou de procédure dans la demande d'interception ou d'autorisation. Il semble qu'il n'ait pas été jugé utile d'exclure en plus des éléments de preuve crédibles et pertinents, compte tenu de la sanction pénale prévue au paragraphe 178.11(1)[22].

La *Loi sur la protection de la vie privée*, qui a été adoptée par la Chambre des communes et est entrée en vigueur le 30 juin 1974, conserve aujourd'hui la même formulation, du moins en ce qui concerne plusieurs de ses aspects les plus importants. Les modifications les plus exhaustives[23] apportées au texte primitif ont été approuvées

19. En effet, selon l'une des propositions, la surveillance électronique autorisée aurait été limitée aux dispositions de la *Loi sur les secrets officiels*, S.R.C. 1970, chap. O-3 ou aux questions relevant de la sécurité nationale.

20. L'alinéa 27(1)*a*) de la *Loi d'interprétation*, S.R.C. 1970, chap. I-23, a également pour effet d'inclure les infractions à option de procédure dans la définition.

21. «[E]t que ce genre d'infractions fait partie d'activités de crime organisé».

22. Voir, par exemple, *Débats de la Chambre des communes*, première session, vingt-neuvième législature, 22-23 Elizabeth II, vol. VIII, 27 novembre 1973, p. 8203 et s.

23. Le projet de loi C-51 a subi la première lecture le 20 avril 1977.

par la Chambre des communes le 18 juillet 1977 et sont entrées en vigueur le 15 octobre 1977. Comme certaines concernaient des points que nous proposons de modifier dans la loi actuelle, quelques brèves observations s'imposent.

B. Le projet de loi C-51

Dans le projet de loi C-51, la définition du mot «infraction» est à nouveau modifiée. Ce terme désigne une série d'incriminations spécifiques[24] et comprend le complot, la tentative ou la complicité après le fait en ce qui concerne les infractions énumérées ainsi que le fait d'inciter ou d'amener une autre personne à commettre ces infractions ou de le lui conseiller. Cette disposition comporte aussi une définition du crime organisé.

Outre l'élargissement de la définition du mot «infraction» à l'article 178.1, la période pour laquelle l'autorisation est accordée et celle du renouvellement de l'autorisation ont été prolongées. Elles sont passées de trente à soixante jours[25]. Cette extension repose essentiellement sur des données selon lesquelles la durée moyenne des interceptions autorisées était d'environ soixante jours[26].

En vertu du projet de loi C-51, les alinéas 178.12(1)*e)* et *e*.1)[27] ont aussi été ajoutés. Ces dispositions rendaient obligatoire la divulgation dans l'affidavit produit à l'appui de la demande, de la profession, si elle est connue, de toutes les personnes dont les communications privées seront interceptées. Des renseignements détaillés sur toute autre demande refusée ou retirée antérieurement et relative à la personne concernée et à l'infraction devraient également être fournis. L'obligation de divulguer la profession des personnes concernées était liée aux propositions tendant à limiter le droit d'intercepter les communications des avocats[28]. Quant à l'exigence de la divulgation des demandes antérieures, elle visait à mettre au moins un frein à la recherche d'un juge favorable[29].

Enfin, l'adoption du projet de loi C-51 apportait des changements importants aux règles du droit de la preuve lorsque des preuves dérivées étaient présentées devant le tribunal. La principale modification, dictée par le souci d'assurer la bonne marche des

24. Les nouvelles infractions, dont l'auteur n'est pas toujours passible d'une peine d'emprisonnement de cinq ans ou plus, comprenaient les actes incriminés par les articles 88, 111, 112, 127, 132, 144 et 340, par les paragraphes 133(1), 185(1) ainsi que les alinéas 159(1)*a*) et 195(1)*a*) du *Code criminel*.

25. Sur ce point, aucune distinction n'a été établie entre les autorisations et les renouvellements.

26. On peut soutenir que même si la modification pouvait faire augmenter la durée de l'immixtion dans la vie privée, les conditions d'obtention de l'autorisation étaient plus sévères que celles qui devaient être remplies pour un renouvellement.

27. L'alinéa 178.12(1)*e*.1) ne faisait pas partie du premier projet de loi.

28. Projet de loi C-51, par. 178.13(1.1) et (1.2).

29. Les modifications relatives à l'avocat sont à la fois trop générales et trop restrictives. D'abord, parce qu'elles ne visent pas les seules communications entre l'avocat et son client et ensuite, parce qu'elles se rapportent à un seul des interlocuteurs, soit «l'avocat». La modification relative à la recherche d'un juge favorable exige seulement que les cas de demande antérieure ou de demande infructueuse soient révélés. Elle vise à empêcher que le juge favorable ne soit choisi en premier lieu.

procès en matière pénale, a soustrait la preuve dérivée à l'application de la règle d'exclusion. Cette preuve devenait recevable à première vue, sous réserve du droit du juge ou du magistrat de l'écarter s'il estimait que son admission ternirait l'image de la justice[30]. Les principes sur lesquels reposait l'admission de la preuve primaire n'ont été modifiés que légèrement afin de préciser que la preuve primaire administrée dans une affaire relative à une infraction autre que celle qui était décrite dans l'autorisation n'était pas de ce fait irrecevable[31].

30. Projet de loi C-51, par. 178.16(1).

31. Par. 178.16(4) du projet de loi C-51 et par. 178.16(3.1) actuel du *Code*. Il n'est pas sûr que cette disposition ait modifié la loi, du moins dans les provinces et les territoires qui ont suivi l'arrêt *R.* v. *Welsh and Iannuzzi (No. 6)*, (1977) 15 O.R. (2d) 1, 32 C.C.C. (2d) 363 (C.A. Ont.).

CHAPITRE DEUX

Arguments en faveur d'une réforme

I. Introduction

Les dispositions de la Partie IV.1 du *Code criminel*[32] ont été présentées par le ministre de la Justice comme une loi visant à protéger la vie privée des personnes. Il était désormais interdit d'intercepter les communications privées, d'en révéler la teneur et de posséder du matériel en vue d'intercepter des communications privées. Toutefois, comme on avait fait valoir des arguments convaincants en faveur de l'utilisation de la surveillance électronique par la police en vue de réprimer le crime, les textes d'incrimination étaient assortis d'un régime prévoyant l'autorisation judiciaire des interceptions.

Depuis l'adoption de la loi, quelques poursuites seulement ont été intentées relativement aux infractions prévues par la Partie IV.1, dont la plupart, sinon la totalité, concernait la possession de dispositifs d'interception. D'ailleurs, dans certains cas il s'agissait de simples dispositifs de détection et non de matériel d'interception sophistiqué. En revanche, l'installation de milliers de tables d'écoute a été autorisée depuis. La Cour suprême du Canada, dans l'arrêt *Goldman* c. *La Reine*[33], a observé qu'il serait plus réaliste de dire que l'objet ou l'effet de la Partie IV.1 est de réglementer la façon d'enfreindre ce droit.

Parmi les arguments pouvant être invoqués à l'appui d'une réforme en matière de surveillance électronique, il est possible de faire deux parts. L'une des préoccupations d'ordre général consiste à se demander de plus en plus si la législation protège, dans les faits, les aspirations légitimes des citoyens en matière de vie privée. La récente adoption de la *Charte canadienne des droits et libertés*[34] fait ressortir encore davantage cette préoccupation. La surveillance électronique est une méthode d'investigation particulièrement envahissante, et elle ne devrait être utilisée que dans des circonstances spéciales lorsque d'autres moyens portant moins atteinte à l'intimité de la vie privée seraient inefficaces. Cette technique devrait être employée avec modération. Au cours des consultations tenues à travers le Canada, personne ne s'est opposé à l'adoption de

32. Pour tous les renvois au *Code criminel*, se référer à S.R.C. 1970, chap. C-34.

33. *Goldman* c. *La Reine*, [1980] 1 R.C.S. 976, p. 994; 51 C.C.C. (2d) 1, p. 15, le juge McIntyre.

34. *Charte canadienne des droits et libertés*, *Loi constitutionnelle de 1982*, telle qu'elle a été adoptée par la *Loi de 1982 sur le Canada* (R.-U.), chap. 11.

la proposition voulant que le recours à la surveillance électronique soit empreint de modération. Toutefois, les avis étaient partagés sur la question de savoir si le régime législatif actuel était appliqué avec modération.

On s'interroge ensuite plus particulièrement sur l'économie de la loi. La Partie IV.1 du *Code criminel* est un texte législatif de nature technique qui pose d'emblée des problèmes d'interprétation. Aussi, bien qu'il soit impérieux d'appliquer les principes de la modération et du respect de la vie privée, n'est-il pas moins important de définir clairement les pouvoirs de la police «... nécessaires à la conduite des enquêtes criminelles, ... sans empiéter de façon abusive ou arbitraire sur les droits et libertés des personnes[35]».

Comme le présent document de travail fait partie du projet de recherche sur les pouvoirs de la police, il convient que nous adoptions aussi une attitude réaliste à l'égard de la loi. Par conséquent, nous nous emploierons principalement à définir les limites de toute atteinte légale au droit à la vie privée. Le présent document de travail porte donc sur l'utilisation de cette méthode d'investigation par la police et non sur les textes d'incrimination. Le renvoi aux infractions est accessoire à l'étude du régime de réglementation et ne fait pas partie de notre mandat dans le cadre du présent document.

Nous sommes d'avis qu'il n'est pas nécessaire de modifier en profondeur le régime législatif actuel. La loi est très récente et, contrairement aux autres aspects concernant les pouvoirs de la police, tend à refléter les valeurs et les principes du vingtième siècle plutôt que ceux du dix-septième, dix-huitième ou dix-neuvième siècle. Par conséquent, les principes de la modération et du respect de la vie privée, la définition des pouvoirs de la police et de l'examen judiciaire sont inscrits en filigrane dans la loi. À notre avis, les problèmes entraînés par le fait que la loi s'écarte de ces principes en raison de la nécessité d'établir un équilibre entre les intérêts en présence, peuvent être résolus dans le cadre de la législation actuelle.

II. Le cadre constitutionnel

L'assujettissement de la surveillance électronique à l'examen prévu à l'article 8 de la *Charte canadienne des droits et libertés*[36], lequel dispose que «[c]hacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives», ne peut plus être contesté en raison de la décision rendue par la Cour suprême du Canada dans l'arrêt *Hunter* c. *Southam Inc.*[37]. Dans cette affaire, le juge en chef Dickson a décidé,

35. Gouvernement du Canada, *Le Droit pénal dans la société canadienne*, Ottawa, Gouvernement du Canada, 1982, p. 69.

36. *Supra*, note 34.

37. *Hunter* c. *Southam Inc.*, [1984] 2 R.C.S. 145, 14 C.C.C. (3d) 97.

en se fondant sur la décision de la Cour suprême des États-Unis dans l'arrêt *Katz* v. *United States*[38], que l'article 8, à l'instar du quatrième amendement de la Constitution des États-Unis, protégeait les expectatives raisonnables des citoyens en matière de vie privée et exigeait qu'un équilibre soit maintenu entre la vie privée du citoyen et le droit du gouvernement d'assurer l'application de la loi[39].

L'adoption du critère de l'expectative raisonnable en matière de vie privée dans l'affaire *Katz* revêt une importance particulière dans le cadre de la présente étude car l'affaire *Katz* concernait l'écoute clandestine. La Cour suprême des États-Unis y a décidé que l'interception des impulsions électroniques était visée par le quatrième amendement, lequel protège les citoyens contre les fouilles, les perquisitions et les saisies abusives. Pour définir les limites de la protection accordée par la Constitution au regard des répercussions de l'ingérence du gouvernement, il est utile de se poser la question suivante : [TRADUCTION] «si la forme précise de surveillance exercée par la police n'était pas soumise aux préceptes de la Constitution, la vie privée et la liberté des citoyens seraient-elles restreintes au point d'être incompatibles avec les principes d'une société libre et démocratique[40]»? Ce type de critère est manifestement applicable en matière de surveillance électronique.

L'autre aspect important de l'affaire *Hunter* c. *Southam Inc.* est la décision de principe de la Cour qui a opté pour l'obtention obligatoire d'une autorisation préalable, tel un mandat, sauf dans les cas où une intrusion sans mandat pourrait être justifiée. De plus, la Cour exige que la détermination de la prépondérance des intérêts en présence soit fondée sur l'appréciation du type d'ingérence projetée et du droit de l'État en cause. Pour l'application ordinaire de la loi, la Cour retient comme critère compatible avec l'article 8 de la Charte l'existence de «motifs probables».

Comme l'a fait observer le juge en chef Dickson, «le droit de l'État de déceler et de prévenir le crime commence à l'emporter sur le droit du particulier de ne pas être importuné lorsque les soupçons font place à la probabilité fondée sur la crédibilité[41]». À notre avis, cette déclaration peut avoir une incidence en matière de surveillance électronique, notamment en ce qui concerne la validité des clauses générales, la définition de l'expression «communication privée», l'installation sans mandat de dispositifs optiques, l'accès aux documents produits lors de la demande et la restriction des interceptions. Dans le seul jugement rendu avant l'affaire *Hunter* dans laquelle il avait été décidé que l'article 8 s'appliquait à l'interception des impulsions électroniques, le juge Ewaschuk avait admis que [TRADUCTION] «le régime législatif canadien transgresserait les exigences constitutionnelles des États-Unis» mais que cela était raisonnable compte tenu du fait que «traditionnellement, en droit canadien, les droits de la société étaient

38. *Katz* v. *United States*, 389 U.S. 347 (1967).

39. *Supra*, note 37, p. 159 (R.C.S.), p. 128 (C.C.C.).

40. A.G. Amsterdam, «Perspectives on the Fourth Amendment», (1974) 58 *Minn. L. Rev.* 349, p. 403.

41. *Supra*, note 37, p. 167-168 (R.C.S.), p. 114-115 (C.C.C.).

jugés prépondérants plus souvent qu'en droit américain[42]». Bien que l'interprétation donnée par le juge Ewaschuk au climat juridique antérieur à l'adoption de la Charte soit peut-être exacte, nous ne pensons pas qu'en vertu de ce texte législatif le droit de la société (c'est-à-dire l'intrusion) l'emporte aussi souvent maintenant sur les droits du particulier. Il convient de noter que le juge en chef Dickson n'a pas associé à la personne, mais à la société, le droit à la vie privée garanti par l'article 8 qui doit être apprécié au regard du droit légitime de l'État d'appliquer la loi. Comme il l'a dit dans le jugement avant d'en arriver à cette conclusion, la constitutionnalité d'une fouille, d'une perquisition et d'une saisie doit être appréciée en fonction surtout de l'effet raisonnable ou abusif sur l'objet de la fouille, de la perquisition ou de la saisie «... et non simplement en fonction de sa rationalité dans la poursuite de quelque objectif gouvernemental valable[43]».

L'adoption de la *Charte canadienne des droits et libertés* exige que la législation soit examinée soigneusement et que nous soyons sensibles aux éventuels arguments invoqués pour démontrer l'incompatibilité de certaines dispositions avec l'article 8.

III. L'équilibre entre le respect de la vie privée et l'application efficace de la loi

Comme nous l'avons vu, la Partie IV.1 du *Code criminel* visait, au moment de son adoption, la suppression de l'écoute clandestine illégale et la surveillance de l'interception des impulsions électroniques par les autorités. Il était clair que l'écoute clandestine et les autres formes d'investigation fondées sur l'interception des impulsions électroniques ne devaient être utilisées qu'exceptionnellement. Mais depuis l'adoption de la Partie IV.1 et depuis les modifications de 1977, en particulier, l'on se demande si l'interception des impulsions électroniques n'a pas été utilisée beaucoup plus fréquemment que prévu au départ et beaucoup plus librement que l'on ne l'avait envisagé. Ces préoccupations ont une double origine : examen habituellement comparatif des données contenues dans les rapports annuels avec les statistiques américaines d'une part et, d'autre part les anecdotes, c'est-à-dire l'utilisation d'une table d'écoute dans des cas considérés sans intérêt ou dans ceux où une autre forme d'investigation, moins attentatoire à l'intimité, aurait pu donner des résultats. Malheureusement, l'article 178.14 portant sur la confidentialité de la demande nous empêche de porter un jugement sur cette question. De toute manière, il serait difficile d'apprécier le bien-fondé de ces craintes, compte tenu du fait que les investigations ne font l'objet d'aucun examen objectif institutionnalisé, mis à part les maigres données fournies par les rapports annuels. L'on ne peut se fier aux preuves de nature anecdotique, en raison de leur grande subjectivité. Ce que le procureur de la défense considère comme l'exercice injustifié du pouvoir d'installer une table d'écoute clandestine, peut être simplement une défaillance de la preuve à l'égard d'un aspect important de l'investigation.

---

42. *R.* v. *Rowbotham*, (1984) 42 C.R. (3d) 164, p. 170 (Haute cour Ont.).
43. *Supra*, note 37, p. 157 (R.C.S.), p. 106 (C.C.C.).

Il est évident que le recours à la statistique comporte des dangers, mais il convient de tenir compte de certaines observations. En dépit du fait que la législation canadienne soit similaire à la législation américaine et qu'elle s'en inspire largement, en réalité le nombre relatif des autorisations accordées est presque vingt fois plus élevé au Canada[44]. À supposer même que la législation américaine soit plus limitative, l'écart est extrêmement important. En outre, bien que l'article 178.13 accorde au juge le pouvoir d'imposer des modalités, celles-ci ne sont à peu près jamais prévues dans les autorisations. En revanche, sans vouloir critiquer outre mesure les fonctionnaires judiciaires, les clauses générales sont libellées en termes de plus en plus vagues et tendent pratiquement à l'universalité dans la plupart des autorisations.

À notre avis, la différence dans l'usage relatif des techniques au Canada et aux États-Unis tient principalement au fait qu'au Canada leur utilisation est beaucoup plus rentable. Il ressort clairement des entrevues avec les autorités chargées d'appliquer la loi aux États-Unis et au Canada que l'écoute clandestine coûte extrêmement cher en temps et en argent aux États-Unis à cause des dispositifs de surveillance et de la paperasserie qu'elle engendre. Bien sûr, il y a peut-être aussi d'autres raisons, telles des dispositions plus sévères en ce qui concerne la divulgation des renseignements qui pousseraient les autorités à abandonner des projets qui les obligeraient à dévoiler l'identité de leurs informateurs, la centralisation du contrôle des demandes, du moins dans le système fédéral, qui tendrait à réduire le nombre de demandes présentées et le fait que certains États interdisent présentement l'écoute clandestine.

Après l'examen qui précède, on constate qu'il est grandement nécessaire de lever le voile sur ce processus. Par conséquent, nous avons abordé bon nombre des dispositions en nous demandant s'il était justifié dans ces cas d'exiger la confidentialité ou le secret. Il va sans dire que des consultations avec la police et le ministère public nous ont grandement aidés à identifier les préoccupations légitimes en matière d'application de la loi et à les apprécier au regard du droit incontesté du public de savoir quelles sont les limites de ce régime compte tenu de ces objectifs en matière d'application de la loi.

---

44. Cette comparaison repose sur les données recueillies en 1981 en vertu de l'article 178.22 du *Code criminel* au Canada et sur celles qui ont été recueillies par le Administrative Office of the United States Courts pour les États-Unis. Au Canada le nombre des autorisations accordées s'élève à 1 059 alors qu'il n'est que de 589 pour les États-Unis. Soulignons que cette proportion est demeurée constante. Voir, par exemple, Louise Savage, *An Analysis of the Federal and Provincial Annual Reports relating to the Use of Court Authorized Electronic Surveillance by Law Enforcement Officials in Canada*, étude non publiée préparée pour la Commission de réforme du droit du Canada, 1979. Les données qui suivent sont tirées de ce document :

	É.-U.	*Canada*
1975	701	1 123
1976	686	1 218
1977	626	1 304

L'écart se maintient en dépit du fait que par suite des modifications apportées en 1977, la durée maximale des autorisations a été portée de trente à soixante jours, alors qu'aux États-Unis la période maximale est demeurée trente jours. Il convient de noter que le nombre de demandes de renouvellement au Canada (205) est «relativement» moins élevé que celui des prorogations accordées aux États-Unis (208).

Un examen de la jurisprudence portant sur la Partie IV.1 du *Code criminel* permet de mettre l'accent sur des domaines précis où cette Partie s'est révélée difficile à appliquer parce que la loi elle-même n'est pas claire et ne contient aucune directive ou parce que la loi est tellement différente des autres lois anglo-canadiennes que la police, les avocats et les juges ont de la difficulté à l'interpréter et à la mettre en œuvre.

Par suite des consultations, d'autres problèmes nous ont été soumis, telles l'interprétation ou l'application de la loi qui, bien qu'elles n'aient jamais fait l'objet de litiges, étaient une cause de préoccupation. Nous avons tenté de résoudre ces problèmes du mieux que nous le pouvions dans nos discussions et nos recommandations.

IV. Le rôle des juges

D'importantes difficultés d'interprétation et de mise en œuvre de la Partie IV.1 du *Code criminel* devaient peut-être être anticipées étant donné que la loi s'inspirait d'un modèle américain. L'exclusion de la preuve avait été adoptée à titre de sanction principale. Les tribunaux canadiens ne sont pas bien au fait d'un tel régime. La règle générale dans le contexte canadien, telle qu'elle a été exprimée dans le jugement *R.* c. *Wray*[45], est au contraire que la preuve est recevable sans égard au mode d'obtention. La seule exception se rapporte aux confessions et le régime prévu ne ressemble pas à la règle de l'exclusion de la preuve obtenue illégalement par l'écoute clandestine. De plus, la preuve dérivée d'une confession obtenue irrégulièrement n'est pas visée par la règle d'exclusion. Un rapport d'analogie pourrait être établi entre le régime de l'écoute clandestine et celui du mandat de perquisition, mais, du moins avant l'adoption de la *Charte canadienne des droits et libertés*, il était clair que les irrégularités dans l'obtention ou l'exécution d'un mandat de perquisition ne rendaient pas irrecevables les éléments de preuve recueillis grâce à la fouille.

Certes, depuis l'adoption de la Charte, la situation est peut-être différente. À l'heure actuelle, il serait téméraire de tenter de prévoir comment les tribunaux régleront le problème du rejet de la preuve en vertu du paragraphe 24(2) dans le cas d'une fouille ou d'une perquisition illégales effectuées en vertu d'un mandat obtenu irrégulièrement. Cependant, il est certain que s'il s'agit d'irrégularités graves dans l'exécution d'un mandat de perquisition, la preuve risque d'être jugée irrecevable[46]. Il est fort possible qu'après l'adoption de la Charte, l'exclusion de la preuve en matière de mandat de perquisition soit régie par des règles similaires à celles qui avaient été prévues par la première loi sur l'écoute clandestine.

45. *Supra*, note 8.

46. *R.* v. *Rao*, (1984) 12 C.C.C. (3d) 97 (C.A. Ont.).

La répugnance du common law à surveiller la police grâce au mécanisme d'une règle d'exclusion a marqué l'interprétation et l'application de la Partie IV.1. Si l'exclusion de la preuve doit être une sanction efficace, les circonstances dans lesquelles la preuve devrait être rejetée doivent être déterminées aussi clairement que possible. C'est d'ailleurs ce que nous tentons de faire dans les recommandations.

L'autre sujet de préoccupation, qui se fait de plus en plus jour, est la réticence des juges, au moment de la présentation de la demande, à considérer que leur rôle en est un de surveillance de l'exercice du pouvoir discrétionnaire de la police. Compte tenu du secret qui entoure le processus de la demande d'autorisation d'intercepter des communications privées, nous n'avons pas de preuve directe de cette réticence. Cependant, nous pouvons invoquer des preuves indirectes relevées dans les données recueillies en vertu de l'article 178.22 du *Code criminel* et par suite d'un examen des autorisations qui, ayant été produites en cour, appartiennent au domaine public.

À nouveau, le rôle traditionnel assumé par les juges canadiens est de ne pas se mêler de l'enquête qui précède la tenue du procès. La seule exception importante, celle de la délivrance d'un mandat de perquisition ou de saisie, a une longue histoire et, comme les études effectuées par la Commission dans ce domaine l'ont révélé, le degré de surveillance judiciaire présentement exercé varie beaucoup[47]. À nouveau, si l'on se plie à la volonté du Parlement qui a décidé qu'une surveillance judiciaire était nécessaire, il semble que les cas dans lesquels les autorisations devraient être accordées et ceux dans lesquels elles ne le devraient *pas* doivent être déterminés et précisés, tout comme le contenu de l'autorisation. Or, en fait, la *Charte canadienne des droits et libertés* appelle la conclusion qu'une surveillance judiciaire est tout à fait indiquée. Le législateur doit reconnaître qu'il est essentiellement injuste de s'attendre à ce qu'un juge, habitué de jouer le rôle de l'arbitre impartial, assume dans les faits un rôle de surveillance sur la poursuite, sans obtenir de lignes directrices très claires sur les limites de son pouvoir. Nous estimons qu'il appartient au Parlement plutôt qu'aux juges de déterminer s'il s'agit d'une intrusion légitime ou d'une immixtion injustifiée dans la vie privée, bien qu'il soit évident que dans chaque cas particulier, la décision ultime reviendra au juge.

Bien qu'au cours des consultations, quantité d'opinions différentes nous aient été soumises sur la précision avec laquelle les critères à appliquer au moment de la demande d'autorisation devraient être établis dans la loi, y compris les modalités, l'exclusion de la preuve, etc., la grande majorité des personnes consultées s'entendait pour dire que la loi pouvait contenir davantage de principes directeurs à l'intention des juges tout en conservant la souplesse nécessaire.

---

47. Commission de réforme du droit du Canada, *Les pouvoirs de la police : les fouilles, les perquisitions et les saisies en droit pénal* [Document de travail 30], Ottawa, Ministère des Approvisionnements et Services, 1983, p. 153 (ci-après appelé le document de travail sur les fouilles, les perquisitions et les saisies). Voir également K.W. Lidstone, «Magistrates, the Police and Search Warrants», (1984) *Crim. L. Rev.* 449.

CHAPITRE TROIS

Recommandations et commentaires

Ce chapitre du document comporte trois volets : l'identification des problèmes, l'examen des solutions et l'exposé des recommandations. Nous n'analysons pas nécessairement la loi actuelle article par article. Nous avons plutôt tenté de résoudre les problèmes qui exigeaient souvent l'analyse de plusieurs articles différents. Cela dit, il faut considérer l'actuelle Partie IV.1 du *Code criminel* comme le cadre dans lequel seront appliquées les recommandations, et les articles pertinents seront toujours mentionnés, sinon cités intégralement.

I. L'application de la Partie IV.1 du *Code criminel*

A. L'infraction

Le principe de la modération exige, en général, que le moyen d'investigation le plus attentatoire à la vie privée ne soit choisi que dans les cas les plus graves ou lorsqu'il est le plus susceptible de donner des résultats tout en empiétant le moins possible sur le droit légitime à la vie privée. L'article 178.1 du *Code* définit actuellement le mot «infraction» par l'énumération d'un grand nombre d'infractions prévues par le *Code criminel* ainsi que certaines infractions créées par d'autres lois fédérales, et par l'intégration d'une disposition générale relative à toute infraction prévue par le *Code* dont l'auteur est passible d'un emprisonnement de cinq ans ou plus, ou qui est une infraction prévue aux articles 3 ou 20 de la *Loi sur les petits prêts*, «dont il existe des motifs raisonnables et probables de croire qu'elle est reliée à un type d'activité criminelle fomentée et organisée par deux ou plusieurs personnes agissant de concert ...[48]». La nécessité pour les fonctionnaires chargés de l'application de la loi d'employer ce genre d'outil est reconnue, car les personnes qui commettent des crimes lucratifs très graves emploieront tout le matériel et les techniques dont elles peuvent disposer[49].

48. *Code criminel*, art. 178.1.

49. Canada, Chambre des communes, *Procès-verbaux et témoignages du Comité permanent de la justice et des questions juridiques*, fasc. 13, 5 juin 1972, p. 13:7.

Aux États-Unis, l'existence du crime organisé a été invoquée pour justifier en quelque sorte l'adoption de la loi (Title III)[50]. Idéalement, la surveillance électronique en vue de réprimer le crime organisé devrait être utilisée comme un mécanisme de collecte de renseignements. La surveillance électronique viserait alors une personne plutôt qu'une infraction et s'exercerait pendant une période indéfinie. En revanche, un tel régime soulève d'importantes difficultés qui ont été reconnues au moment de l'adoption de la Partie IV.1. Le problème le plus évident peut-être est la difficulté de définir de façon satisfaisante l'expression «crime organisé». L'article 178.1 se borne à peu près à définir le complot. En outre, la Commission a dénoncé les empiétements qui ont pour unique but de recueillir des renseignements et a fait remarquer que «[l]e droit, en général, doit restreindre la justification de ces atteintes aux seuls cas où la perpétration de l'infraction a été amorcée[51]». Nous estimons que ce principe est applicable à la surveillance électronique au même titre qu'aux fouilles, aux perquisitions et aux saisies. Nous ne sommes pas convaincus que ce principe puisse être sacrifié sous prétexte de lutter contre le crime organisé. À notre avis, les préoccupations relatives à la menace grave que représente pour la vie et les biens le crime organisé et à la difficulté de mener à bien une enquête sur cette activité peuvent trouver une solution efficace dans un régime fondé sur la perpétration d'une infraction précise et permettant la délivrance d'une autorisation d'enquêter sur un complot en vue de commettre une telle infraction (comme c'est le cas dans la loi actuelle).

En outre, bien que l'essentiel des discussions concernant la Partie IV.1 ait porté sur l'utilité de l'écoute clandestine comme moyen de combattre le crime organisé, il est évident que cette technique a aussi servi à d'autres fins. Nous estimons donc qu'il ne convient pas d'axer le régime de l'écoute clandestine sur l'identification des infractions commises par des organisations criminelles. En effet, nous ne voyons pas pourquoi certaines infractions peu importantes seraient visées par ce régime sous prétexte qu'elles relèvent du crime organisé ni pourquoi certains crimes graves en seraient exclus parce qu'ils ne sont pas d'ordinaire le fait d'organisations criminelles. Nous ne sommes pas non plus convaincus que le nombre de demandes d'autorisation présentées antérieurement au sujet d'une infraction précise permette de décider s'il faut faire figurer cette infraction dans la Partie IV.1. Nous admettons évidemment que le nombre élevé d'autorisations accordées relativement à certaines infractions est une mesure de l'utilité de l'écoute clandestine pendant l'enquête. En revanche, le nombre assez peu élevé d'autorisations accordées relativement à des enlèvements ou à des meurtres ne signifie pas qu'il ne soit pas essentiel, le cas échéant, d'avoir recours à l'écoute clandestine pour faire avancer l'enquête.

Bien que l'énumération des infractions nous semble être la seule solution, à notre avis, il reste du moins possible d'adopter des critères régissant l'adjonction d'infractions à la liste. Dans son quatrième rapport, le Comité permanent de la justice et des questions juridiques a proposé que l'infraction soit un crime grave qui constitue une menace pour

50. American Bar Association, projet sur *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance*, version provisoire, juin 1968.

51. Document de travail sur les fouilles, les perquisitions et les saisies, *supra*, note 47, p. 153.

la vie et le bien-être individuel et collectif au point que la protection contre une activité antisociale doive l'emporter sur la protection de l'intimité de la vie privée[52]. Dans l'ouvrage intitulé *Standards for Criminal Justice*, l'American Bar Association a retenu la norme suivante : l'infraction est grave en elle-même ou elle caractérise les activités d'un groupe[53]. L'intérêt du dernier critère est de rappeler l'utilité de l'écoute clandestine en matière d'investigation. En effet, il semble raisonnable de penser que les infractions qui caractérisent les activités de groupe, et donc nécessitent une communication entre leurs membres, se prêtent mieux à l'écoute clandestine qui permettrait alors de recueillir un nombre appréciable d'éléments de preuve. Le critère retenu par l'American Bar Association peut être illustré, d'une part, par le meurtre qui est une infraction grave en elle-même, et d'autre part, par le jeu qui caractérise les activités d'un groupe. À notre avis, le recours à l'écoute clandestine dans le cas de ces deux infractions devrait à juste titre être permis : dans le cas du meurtre, en raison de sa gravité évidente et dans le cas du jeu parce qu'il est très probable que la surveillance électronique *exercée correctement* est une méthode qui permettrait de recueillir des preuves pertinentes tout en réduisant au minimum les atteintes portées au droit légitime à la vie privée dans des circonstances où il aurait été difficile de détecter l'infraction autrement. Dans le régime que nous proposons, la loi disposerait que pour ces deux types d'infraction il doit y avoir une probabilité raisonnable d'obtenir des éléments de preuve utiles et, en ce qui concerne les infractions moins graves, que le degré d'immixtion doit être réduit.

On a fait valoir que la définition du mot «infraction» peut être rationalisée en énonçant simplement que l'autorisation sera accordée lorsqu'il s'agira de la commission de tout acte criminel comme on l'a fait dans le cas des mandats de perquisition, lesquels peuvent être délivrés relativement à *toute* infraction. Nous ne sommes pas convaincus qu'une telle rationalisation soit souhaitable ni qu'il soit opportun d'établir un parallèle avec les conditions de délivrance d'un mandat de perquisition. Bien que les fouilles ou perquisitions effectuées au domicile ou au bureau d'une personne portent sans aucun doute atteinte à son droit à la vie privée, cette immixtion et celle qui est envisagée lors d'une surveillance électronique sont de nature différente. Même les opérations de fouilles de grande envergure durent au plus une ou deux journées. Elles visent à recueillir des preuves existantes ou des marchandises de contrebande dont on sait non seulement qu'elles seront très probablement trouvées mais qu'elles le seront à l'endroit où l'on cherche à perquisitionner. En revanche, l'écoute clandestine est autorisée en raison même d'un manque de preuves. Elle n'a pas pour objet premier de mettre au jour des marchandises de contrebande ou des éléments de preuve. Certes, on s'attend à ce que des éléments de preuve soient obtenus, mais il ne s'agira pas d'objets ni de documents. Ils prendront plutôt la forme d'idées exprimées par les personnes faisant l'objet de l'écoute. Il n'est possible d'établir un parallèle entre le mandat de perquisition et la surveillance électronique que sur un seul point : les infractions moins graves devraient faire l'objet d'une interception seulement lorsqu'il est très probable que cette opération

52. Canada, Chambre des communes, Comité permanent de la justice et des questions juridiques, *Quatrième rapport*, 1970.

53. American Bar Association, *Standards for Criminal Justice*, 2e éd., Boston, Little, Brown and Company, 1986.

permettra de recueillir des éléments de preuve. Pour ramener l'analogie à de justes proportions, il suffit de se demander si un juge autoriserait sciemment la perquisition quotidienne dans un lieu pendant une période de trente à soixante jours, durée pour laquelle sont accordées la plupart des autorisations, sans qu'il soit tenu compte du degré de gravité de l'infraction ni de la certitude d'obtenir des éléments de preuve ou des marchandises de contrebande.

Les infractions prévues par le régime de l'écoute clandestine lui-même, c'est-à-dire les infractions créées par les articles 178.11 et 178.18 du *Code criminel* constituent clairement des arguments à l'encontre de l'application d'une double norme. Après consultation des rapports annuels présentés en application de l'article 178.22 du *Code criminel*, que nous avons pu obtenir, il nous est impossible de conclure que ces dispositions ont été invoquées. En revanche, l'inclusion de ces infractions à l'article 178.1 est une mesure de l'engagement du gouvernement en matière de droit à la vie privée car elles sont véritablement à la base de la législation : l'écoute clandestine non autorisée ou non consensuelle devrait être illégale.

Enfin, nous estimons que le critère relatif à l'activité d'un groupe doit être employé avec modération. Il faudrait qu'il soit très probable, du fait de la nature même de l'infraction, que des éléments de preuve ne puissent être obtenus que de cette façon. De plus, les infractions qui ne sont pas bien définies dans le *Code* et à l'égard desquelles l'investigation peut porter atteinte aux droits fondamentaux, telle la liberté d'expression, ne devraient pas figurer dans la liste des infractions.

Nous recommandons des modifications relativement mineures à la liste actuelle des infractions pour lesquelles une autorisation peut être accordée. Notre principale recommandation, l'élimination du critère relatif aux activités des organisations criminelles, a été largement acceptée car la plupart des personnes consultées se sont accordées pour dire que cette expression était impossible à définir et encore plus difficile à appliquer et qu'elle ouvrait la porte à tous les abus.

RECOMMANDATIONS

1. Les infractions pour lesquelles une autorisation d'intercepter des communications privées peut être obtenue devraient continuer de figurer sur une liste dressée à cette fin. Les infractions suivantes devraient être rayées de l'actuelle liste de l'article 178.1 : *Code criminel* — art. 58 (faux ou usage de faux, etc.), al. 159(1)*a*) (documentation pornographique), al. 195(1)*a*) (proxénétisme), art. 281.1 (encouragement au génocide), art. 314 (vol de courrier), art. 331 (menaces par lettres), art. 339 (emploi du courrier pour frauder); *Loi sur l'accise* — art. 158 et 163 (distillation ou vente illégale d'eau-de-vie).

2. Il y aurait lieu d'adjoindre à la liste les infractions prévues par le *Code criminel* qui suivent : al. 195(1)*b*), *c*), *d*), *h*) et *i*) (proxénétisme), art. 305.1 (taux d'intérêt criminel)[54], art. 381.1 (menaces de commettre une infraction contre une personne jouissant d'une protection internationale)[55].

3. La définition du crime organisé devrait être retirée de la liste des infractions visées, mais il devrait être possible d'obtenir une autorisation relativement aux enquêtes sur les complots, les tentatives et la complicité après le fait, en ce qui a trait à une infraction désignée, ou le fait de conseiller à une personne de commettre une telle infraction, de l'y amener ou de l'y inciter.

B. Les communications privées

Le choix des communications à protéger est un point essentiel dans l'élaboration d'un régime législatif en matière de surveillance électronique. La définition de la communication privée est fondée sur la valeur inhérente de la protection de la vie privée. Bien que la Partie IV.1 traite de l'usage des éléments de preuve obtenus par suite de l'interception illégale d'une communication privée si une partie consent à ce qu'elle soit produite en preuve (al. 178.16(1)*b*) du *Code criminel*), il est incontestable que l'objet principal de la loi était à la fois de régir l'utilisation légale de la surveillance électronique et d'en incriminer l'utilisation illégale. Actuellement, la communication privée est définie comme suit : «toute communication orale ou télécommunication faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par une personne autre que la personne à laquelle il la destine[56]».

Bien que seules les communications dont l'auteur peut raisonnablement s'attendre à ce qu'elles demeureront privées nécessitent l'instauration d'un régime législatif, le recours sans cesse croissant à la surveillance électronique par les organismes de l'État

54. L'ajout de cette infraction nécessite peut-être certaines explications. La suppression de l'expression «crime organisé» enlève toute référence à la *Loi sur les petits prêts*, S.R.C. 1970, chap. S-11. Par cette référence, le législateur entendait lutter contre le prêt usuraire, infraction souvent associée au véritable crime organisé et à l'extorsion. Ce domaine est aujourd'hui visé par le nouvel article 305.1 du *Code criminel* et comme l'extorsion (art. 305), il devrait s'agir d'une infraction pour laquelle une autorisation peut être demandée. Les victimes sont particulièrement vulnérables, et l'application efficace de la loi peut être assujettie à l'existence d'éléments de preuve susceptibles d'être obtenus par l'interception des communications.

55. Le projet de loi C-18 qui a été adopté par le Parlement proposait en son article 22 certaines modifications à l'article 178.1 du *Code criminel*, qui rejoignent en partie cette recommandation. Cette disposition ne supprime que les infractions incriminées par l'article 331 et l'alinéa 195(1)*a*) (proxénétisme), ce dernier étant cependant remplacé par un renvoi au paragraphe 195(1) (proxénétisme). Comme le lecteur le constatera, nous recommandons aussi que des modifications relatives à l'article 195 soient apportées. Toutefois, nous proposons plutôt de remplacer le renvoi à l'alinéa 195(1)*a*) par un renvoi à d'autres dispositions incriminant des actes suggérant l'emploi de la force ou de la contrainte. Certaines des infractions visées au paragraphe 195(1) ne sont tout simplement pas assez graves pour figurer dans la liste de l'article 178.1.

56. *Code criminel*, art. 178.1.

ou la perception grandissante de ce phénomène, ouvre une perspective peu réjouissante : il n'est pas déraisonnable pour une personne de penser que son téléphone a été mis sur écoute. Si cette tendance s'accentuait, l'écoute téléphonique pourrait échapper à tout contrôle car les autorités n'auraient qu'à invoquer les appréhensions raisonnables du public concernant l'usage généralisé des dispositifs d'écoute téléphonique[57]. Cette opinion a été exprimée par le juge Brooke, dans une récente décision de la Cour d'appel de l'Ontario[58]. Dans son jugement, le juge Brooke fait observer que lorsqu'il a été prouvé que l'intimé savait que les risques d'interception de ses communications téléphoniques étaient bien réels, il est douteux que l'on puisse dire que ces communications avaient été faites dans des circonstances telles que leur auteur pouvait raisonnablement s'attendre à ce qu'elles ne soient pas interceptées par une autre personne que celle à laquelle il les destinait.

Toutes ces considérations nous éloignent des buts poursuivis par l'adoption de la Partie IV.1 du *Code*. Exception faite des «criminels», une foule de gens vivent dans la crainte perpétuelle que leur téléphone soit mis sur écoute. En 1974, le professeur Amsterdam, dans un autre ordre d'idées, s'est penché sur la question de lier la réglementation des atteintes à la vie privée aux attentes raisonnables subjectives (et non pas justifiées) de la personne en la matière. Il a conclu [TRADUCTION] «qu'il ne faut évidemment pas tenir compte des attentes réelles et subjectives en ce qui concerne le droit à la vie privée ... pour déterminer le champ d'application de la garantie offerte par le quatrième amendement. Elles n'ont aucune incidence sur les revendications fondées sur le quatrième amendement[59]».

Le droit légitime du public à la protection de la vie privée pourrait être gravement atteint si la définition de l'expression «communication privée» n'est pas modifiée. Il faudrait dans le cadre d'une nouvelle définition tenir compte du fait que de plus en plus de gens savent que l'écoute téléphonique existe et préciser qu'une partie à une communication «privée» s'attend tout de même raisonnablement à ce que son intimité soit respectée parce que sa seule crainte concerne la possibilité d'une interception légalement autorisée.

Un autre problème lié à la définition de l'expression «communication privée» a fait l'objet d'un examen dans le jugement *Goldman* c. *La Reine*[60] rendu par la Cour suprême du Canada. Dans cette affaire, on a fait valoir que les communications qui avaient été interceptées grâce à un micro-émetteur portatif n'étaient pas des communications privées puisque le policier, auteur de la communication, savait que la conversation serait interceptée. Le juge McIntyre a réglé le problème de façon pragmatique et a décidé que «l'auteur» est la personne «qui fait la remarque ou série de remarques que le ministère public cherche à produire en preuve». Le juge a allégué ceci :

---

57. *R.* v. *Carothers*, [1978] 6 W.W.R. 571 (Cour de comté C.-B.).
58. *R.* v. *Samson*, (1983) 9 C.C.C. (2d) 194, p. 204 (C.A. Ont.).
59. A.G. Amsterdam, *loc. cit. supra*, note 40, p. 384.
60. *Supra*, note 33.

> lorsqu'un policier est partie à une conversation avec un suspect, sachant qu'elle est interceptée électroniquement, et entend le suspect faire les déclarations incriminantes attendues et utiles à la preuve à charge, je ne peux considérer que le policier est l'auteur des déclarations mêmes qu'il cherchait à obtenir[61].

Sans d'aucune façon diminuer l'importance des difficultés soulevées par le problème d'interprétation que devait résoudre la Cour, il n'est pas d'emblée évident que l'économie de la loi favorise l'interprétation adoptée par elle. Dans l'affaire *Goldman* elle-même, la seule conséquence de l'application ou de la non-application des dispositions de la Partie IV.1 serait que des complications d'ordre procédural devraient être aplanies pour que l'enregistrement de la conversation soit admis en preuve si le policier n'est pas libre, ni en mesure de témoigner sur le contenu de la conversation. Le droit à la *vie privée* dans l'affaire *Goldman* est une notion très abstraite dans de telles circonstances. La question principale ne se rapporte pas à la surveillance électronique. Ce problème est seulement accessoire à la question plus large du recours aux policiers. La seule raison justifiant véritablement l'application de la Partie IV.1 dans l'affaire *Goldman* est la communication de la preuve, c'est-à-dire l'application des dispositions du paragraphe 178.16(4) relatif à l'avis de l'intention de produire une preuve. Le principe régissant une telle situation devrait favoriser l'observation de la procédure d'obtention d'une autorisation lorsqu'il en va réellement du droit à la vie privée. En outre, il devrait être susceptible d'une application pratique. Même la règle élaborée dans l'affaire *Goldman* présente des lacunes sur ce point car la Cour doit morceler la conversation afin d'obtenir des «communications distinctes». À notre avis, la Partie IV.1 devrait protéger l'intimité des conversations et non les communications individuelles. Le principe prépondérant en la matière doit favoriser l'adoption d'une règle simple, pratique et facilement applicable. La solution la plus facile consiste à définir l'expression «communication privée» de façon que l'intégralité des conversations dont l'une ou l'autre des parties s'attendent à ce qu'elles demeurent privées soit visée. Le problème du micro-émetteur peut être réglé séparément en même temps que la question relative à l'admissibilité de la preuve et aux dispositions créant des infractions.

Cependant, nous craignons que cette nouvelle définition ne pose des problèmes en ce qui concerne les prisons et autres lieux de détention, et les prises d'otages. En vertu de la loi actuelle, lorsque les prises d'otages sont publiques et que les protagonistes se servent du téléphone pour négocier avec la police ou pour communiquer avec d'autres personnes, il semble que la nouvelle définition ne soulève aucun problème. En effet, il ne serait pas raisonnable de croire que de telles communications ne sont pas surveillées[62], quoique cette opinion puisse découler du fait que l'on soit convaincu que cette surveillance est effectuée par suite de la délivrance d'une autorisation judiciaire. Tout le dilemme est là : les prises d'otages constituent-elles une menace pour la vie et la sécurité des autres si grave et pressante qu'une exemption spéciale doive être prévue dans la définition proposée de l'expression «communication privée»? Dans ce cas, la police pourrait à sa guise intercepter les communications dans ces circonstances sans qu'il soit

61. *Id.*, p. 995 (R.C.S.), p. 16 (C.C.C.).

62. Voir *R.* v. *Gamble and Nichols*, (1978) 40 C.C.C. (2d) 415, p. 424 (C.S., D.A. Alb.).

nécessaire d'obtenir l'autorisation de la Cour. À notre avis, l'importance du respect de la vie privée est considérablement diminuée lorsque les dangers qui pèsent sur les personnes sont si graves. Il convient de rédiger soigneusement le texte législatif pour veiller à ce que les communications de l'auteur d'une prise d'otages avec l'extérieur ne soient pas visées, comme avant, par la définition de l'expression «communication privée». Nous estimons que la recommandation 4 atteint cet objectif.

L'autre problème se rapporte aux communications dans les prisons. Pour des raisons de sécurité, les communications des prisonniers avec le monde extérieur sont surveillées par le personnel de l'établissement. L'une des façons de justifier cette méthode est de coller des étiquettes sur le téléphone de l'établissement annonçant que la conversation est interceptée ou pourrait l'être[63]. En vertu de la définition actuelle, il ne s'agirait pas de l'interception d'une communication privée. Une telle interception serait donc soustraite aux dispositions de la Partie IV.1 et ne serait pas illégale. En revanche, en vertu de la définition que nous proposons, il s'agirait bien de l'interception d'une communication privée puisque l'interlocuteur de l'extérieur pourrait raisonnablement penser que la conversation n'est pas interceptée. Si le problème est abordé de cette façon, la solution consiste non pas à déformer la définition de l'expression «communication privée» mais à rendre de telles interceptions légales par la voie d'une modification de l'article 178.11.

La question de savoir si la Partie IV.1 s'applique à l'interception d'une conversation sans l'aide d'un dispositif électronique prête à controverse. Dans l'arrêt *R.* v. *Beckner*[64], la Cour a jugé que la Partie IV.1 ne s'appliquait pas. Cependant, dans une décision antérieure, *R.* v. *Boutilier and Melnick*[65], l'opinion contraire avait été retenue. À notre avis, la conclusion de l'arrêt *Beckner* est correcte. Bien que l'on puisse soutenir qu'il est nécessaire de réglementer toute ingérence de la police dans la vie privée, le débat devient frivole à un certain point de la discussion. Ce qui est interdit par un régime en matière de respect de la vie privée est tout aussi important que ce qui est permis. Exiger la réglementation de l'admissibilité des conversations entendues implique que de telles conduites seront illégales sauf dans certaines circonstances bien déterminées. Cela suppose un changement radical de la conduite de la plupart des gens, même dans les activités quotidiennes ordinaires[66].

L'inclusion du mot «télécommunication» dans la définition de la communication privée soulève un problème connexe hautement technique. Dans la *Loi d'interprétation*, le mot «télécommunication» est défini à l'article 28 comme suit : «toute transmission, émission ou réception des signes, signaux, écrits, images ou sons, ou de renseignements de quelque nature que ce soit, par fil, par radio, par un procédé visuel ou un autre procédé électromagnétique».

---

63. Voir *R.* v. *Rodney*, (1984) 12 C.C.C. (3d) 195 (C.S. C.-B.).
64. *R.* v. *Beckner*, (1978) 43 C.C.C. (2d) 356 (C.A. Ont.).
65. *R.* v. *Boutilier and Melnick*, (1976) 35 C.C.C. (2d) 555 (C.S. N.-É.)
66. *Op. cit. supra*, note 4, p. 44.

La même définition est également employée dans les articles 287 (vol de service de télécommunication) et 287.1 (possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunication) du *Code criminel*. Cette définition est très large et l'on s'est demandé si elle visait l'interception des communications transmises à des dispositifs payeurs, lesquels peuvent être visés par la définition de l'expression «communication privée».

Cependant, la définition pourra également s'appliquer à l'usage des dispositifs parfois appelés enregistreurs à plume qui n'exigent aucune conversation, seulement la composition d'un numéro sur le cadran téléphonique. Les autorités chargées d'appliquer la loi s'accordent pour dire que ces dispositifs ne sont pas visés par la loi et devraient pouvoir être utilisés sans qu'il soit nécessaire d'obtenir une autorisation. En réalité, un tel dispositif pourrait servir à préparer le matériel nécessaire à l'obtention d'une autorisation car il peut aider les policiers à dépister les auteurs d'un complot présumé. Il est évident que de tels dispositifs ne sont pas visés par la loi américaine (Title III[67]), qui mentionne les seules interceptions «sonores» des communications privées. Le recours sans autorisation à de tels dispositifs ne porte pas non plus atteinte au quatrième amendement car une personne ne peut s'attendre raisonnablement à ce que les numéros composés demeurent confidentiels[68]. À notre avis, rien ne justifie que soient visés par la Partie IV.1 les enregistreurs à plume et autres dispositifs connexes (tels les voyants à diode lumineuse employés pour retracer le numéro de l'interlocuteur après que celui-ci a raccroché). Ces dispositions visent principalement à protéger l'intimité des communications, c'est-à-dire les conversations entre les personnes. De tels dispositifs ne portent pas atteinte à l'intimité des communications. En outre, l'espoir de préserver la confidentialité des numéros de téléphone composés ou celle des appels reçus est mince. Il suffira d'apporter une légère modification à la définition de l'expression «dispositif électromagnétique, acoustique, mécanique ou autre» pour remédier à cette lacune de la loi.

RECOMMANDATIONS

4. L'expression «communication privée» devrait être définie de la façon suivante :

> **Toute communication orale ou télécommunication faites dans des circonstances telles que toute personne y participant peut raisonnablement s'attendre à ce qu'elles ne soient pas interceptées par le moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre.**

---

67. U.S., *Omnibus Crime Control and Safe Streets Act of 1968*, Title III, Act of June 19, 1968, Pub. L. No. 90-351 (ci-après appelé Title III). Voir aussi J.G. Carr, *The Law of Electronic Surveillance*, New York, Clark Boardman, 1977, p. 74.

68. *Smith* v. *Maryland*, 442 U.S. 735 (1979). Voir, cependant, *People* v. *Sporleder*, 666 P.2d 135, Colo. (1983).

5. Une communication devrait être considérée comme privée même si une personne qui y participe croit qu'elle pourrait faire l'objet d'une autorisation accordée par un tribunal à un organisme chargé de l'application de la loi.

6. Le paragraphe 178.11(2) devrait être modifié par l'adjonction de l'alinéa *e*) comme suit :

> **à une personne qui surveille à des fins de sécurité des communications faites par les détenus d'une prison définie par la *Loi sur les prisons et les maisons de correction*, S.R.C. 1970, chap. P-21 et d'un pénitencier défini par la *Loi sur les pénitenciers*, S.R.C. 1970, chap. P-6, lorsque le fait qu'une telle surveillance peut être effectuée est dévoilé dans une annonce placée bien en vue à l'endroit où la communication peut être faite.**

7. La définition de l'expression «dispositif électromagnétique, acoustique, mécanique ou autre» devrait être modifiée comme suit :

> **«dispositif électromagnétique, acoustique, mécanique ou autre» désigne tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une communication privée, mais ne comprend pas un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale, ni un dispositif tels l'enregistreur à plume, le décodeur d'impulsions multifréquences, le voyant à diode lumineuse ou autre dispositif similaire servant à identifier le numéro de téléphone composé ou l'interlocuteur et à obtenir l'heure et la date de l'appel téléphonique sans permettre l'interception des mots ni de tout autre renseignement.**

C. Les dispositifs optiques

Le problème de l'utilisation des dispositifs optiques est étroitement lié à la définition de la communication privée que nous venons d'examiner et donc, à l'application de la Partie IV.1.

Il semble clair que l'actuelle Partie IV.1 ne vise pas les dispositifs optiques[69]. Contrairement à la position qu'elle a prise dans son rapport intitulé *Criminal Investigation*[70], la Law Reform Commission of Australia a souligné dans son document de travail publié en 1980 que l'utilisation des dispositifs optiques posait de graves problèmes en matière de respect de la vie privée. Elle déplore [TRADUCTION] «qu'antérieurement il suffisait de prendre des mesures simples pour protéger sa vie privée du

69. *R.* v. *Biasi (No. 3)*, (1981) 66 C.C.C. (2d) 566 (C.S. C.-B.).

70. Law Reform Commission of Australia, *Criminal Investigation* [Report No. 2], Canberra, Australian Government Publishing Service, 1975.

regard indiscret des tiers. Aujourd'hui, ces mesures ne conviennent plus car les développements technologiques ne sont pas restreints aux dispositifs d'écoute et d'interception[71]».

Nous n'ignorons pas que d'importantes questions portant sur le respect de la vie privée *risquent* d'être soulevées dans ce domaine. Toutefois, jusqu'ici les renseignements recueillis ne démontrent nullement que l'utilisation des dispositifs optiques ait entraîné de graves abus, ni causé des immixtions injustifiables dans la vie privée. L'adoption d'une loi à portée générale porterait gravement atteinte au droit de propriété. On ne peut légitimement empêcher les propriétaires de banques, d'épiceries et autres établissements semblables d'utiliser des caméras pour se protéger contre toute conduite illégale. Ces dispositifs servent aussi à enregistrer les transactions illégales conclues entre des suspects et des policiers. Tout comme dans le cas des micro-émetteurs, l'utilisation des dispositifs optiques ne pose que des problèmes d'ordre très théorique en matière de droit à la vie privée. Mentionnons enfin l'usage de dispositifs tels les jumelles et les téléscopes. La Cour suprême des États-Unis a examiné cette question dans le cadre de l'application des garanties offertes par le quatrième amendement contre les fouilles, les perquisitions et les saisies abusives. Dans l'affaire *United States* v. *Knotts*[72], la Cour, qui avait étudié les conséquences de l'utilisation d'un émetteur transmettant un signal électronique et permettant aux policiers de suivre le véhicule du suspect, a fait remarquer que [TRADUCTION] «les dispositions du quatrième amendement n'interdisaient pas aux policiers d'augmenter les capacités sensorielles dont ils avaient été dotés à leur naissance grâce aux moyens que la science et la technologie mettaient à leur disposition dans cette affaire[73]».

À notre avis, beaucoup d'autres travaux de recherche devront être effectués sur les types et les possibilités offertes par les dispositifs actuellement utilisés avant qu'une législation exhaustive puisse être adoptée. Cependant, sur un point précis les questions sont claires et le droit à la vie privée est nettement en jeu : l'entrée clandestine dans un lieu privé par des représentants du gouvernement en vue de mettre en place des dispositifs optiques. Nous proposons de la réglementer au même titre que l'entrée clandestine en vue d'installer des dispositifs d'écoute (micro) et d'attendre les résultats de la recherche pour répondre aux autres questions. Nous ne nous sentons pas prêts à résoudre les diverses questions politiques que peut soulever l'adoption d'un critère plus large, telle la réglementation des dispositifs dans tous les lieux où une personne peut raisonnablement s'attendre à ce que son intimité soit respectée.

En outre, parce que nous entendons réglementer l'entrée clandestine en vue de l'installation de dispositifs d'écoute, le fait de ne pas réglementer les dispositifs optiques

71. *Op. cit. supra*, note 4, p. 64-65.

72. *United States* v. *Knotts*, 103 S.Ct. 1081 (1983).

73. *Id.*, p. 1086. En revanche, les dispositifs électroniques comme un émetteur ne peuvent être utilisés pour obtenir des renseignements lorsque la surveillance visuelle n'aurait pas été autorisée, par exemple dans une habitation privée (voir *United States* v. *Karo*, 104 S.Ct. 3296 (1984)), en dépit du fait que l'émetteur soit un moyen moins attentatoire à la vie privée qu'une opération de perquisition de grande envergure.

constituerait une lacune qui permettrait, même aux autorités chargées de l'application de la loi, de faire indirectement ce que la loi interdit.

. En conclusion, nous tenons à préciser que nous ne cherchons nullement à diminuer l'importance des problèmes créés par l'usage à des fins d'application de la loi des dispositifs optiques, même avec le consentement du propriétaire. Qu'il s'agisse ou non d'un usage judicieux des ressources, nous ne pouvons que suggérer, en guise de recommandation, que tout le domaine de la surveillance optique clandestine doive faire l'objet d'un examen[74].

RECOMMANDATIONS

8. Devrait constituer une infraction le fait d'entrer dans un lieu privé, sans autorisation judiciaire ni consentement du propriétaire ou de l'occupant légitime, afin d'y installer un dispositif optique.

9. L'autorisation d'installer un dispositif optique devrait pouvoir être obtenue sur demande présentée à un tribunal, mais aux mêmes conditions qu'une autorisation en vue de l'installation d'un dispositif d'écoute par une entrée clandestine.

10. L'expression «dispositif optique» devrait, pour l'instant, désigner tout dispositif ou mécanisme susceptible de permettre l'observation visuelle clandestine de personnes ou d'objets.

D. L'interception de communications privées à l'étranger

L'un des autres problèmes posés par l'application de la Partie IV.1 du *Code criminel* est celui de l'interception des communications privées faite à l'étranger.

Plusieurs décisions récentes rendues par les tribunaux de la Colombie-Britannique ont soulevé le problème de la réglementation des éléments de preuve recueillis par suite de l'interception de communications privées faite à l'étranger. Cette question relève du droit de la preuve puisqu'il est admis que le droit substantif canadien n'a pas d'application à l'étranger et ne peut régir les conversations échangées entièrement à l'étranger. La Cour suprême de la Colombie-Britannique a rendu à ce sujet des jugements contradictoires. D'une part, des communications privées interceptées à l'étranger ne sont pas admissibles s'il n'a pas été prouvé qu'elles ont été interceptées légalement selon la loi du pays dans lequel elles ont été interceptées[75] et, d'autre part, la Partie IV.1 ne s'appliquant pas à une telle communication, leur admissibilité est par conséquent

74. Voir *U.S.* v. *Torres*, 36 Cr.L. 2301 (7th Cir.), p. 2302 (19 décembre 1984).

75. Voir *R.* v. *Bengert (No. 8)*, (1979) 15 C.R. (3d) 37 (C.S. C.-B.) et *R.* v. *Bengert (No. 9)*, (1979) 10 B.C.L.R. 199, 15 C.R. (3d) 40 (C.S. C.-B.).

régie par le droit général de la preuve[76]. Une troisième solution consisterait à exiger que l'interception ait été faite selon les normes canadiennes. Il convient de noter que cette dernière solution entraînerait l'exclusion des éléments de preuve recueillis dans de nombreux pays tel le Royaume-Uni[77] où l'écoute téléphonique est autorisée par le *Home Secretary* et non par un juge. Dans ce cas, ni l'application des principes de la procédure pénale ni la protection du droit à la vie privée ne nous sont d'aucun secours pour trouver la solution. Les Canadiens qui choisissent de faire affaires à l'étranger doivent s'attendre à ce qu'elles soient régies par les gouvernements étrangers et, peut-être, à ce que ceux-ci s'immiscent, comme ils l'entendent, dans leur vie privée.

Les autres principes pertinents sont le respect des engagements internationaux, l'économie, la clarté, ainsi que l'administration juste et efficace de la justice. À notre avis, il serait en pratique très difficile et peu respectueux des engagements internationaux d'imposer le régime canadien aux gouvernements étrangers (troisième solution).

L'argument invoqué à l'appui de la troisième solution est que puisque l'accusé est jugé par les tribunaux canadiens, dans le respect de la procédure canadienne, la production des éléments de preuve doit être conforme aux normes d'admissibilité canadiennes. Cet argument est similaire à la règle qui prévaut en matière de confession. En effet, les tribunaux canadiens ne recevant pas une confession obtenue par la torture, à supposer même que de tels procédés soient légaux dans l'État où la confession a été obtenue, ils ne devraient pas accepter non plus les règles de cet État dans d'autres circonstances. Lorsque l'accusé est jugé au Canada, les règles de la preuve du Canada doivent être considérées comme une norme minimale. Sinon, le droit à l'égalité pourrait être invoqué. Prenons l'exemple de deux accusés jugés au Canada dont les conversations ont été interceptées par les mêmes moyens. Dans l'un des cas, l'interception a été faite au Canada, mais elle ne respecte pas les dispositions de la Partie IV.1 du *Code criminel*. Cette conversation n'est donc pas recevable. Dans l'autre cas, la conversation a été interceptée à l'étranger selon les règles de l'État où elle a été interceptée, lesquelles sont moins rigoureuses que les nôtres. Ces conversations seront admissibles.

Nous ne sommes pas convaincus que la logique de ces arguments soit irrésistible au point de rendre impérieuse l'adoption de la troisième solution.

Le rapport d'analogie établi avec la règle d'inadmissibilité des confessions ne fournit pas véritablement de principes de base en matière d'écoute clandestine. En premier lieu, les confessions sont exclues, sauf s'il s'agit de déclarations volontaires afin a) de s'assurer qu'elles sont dignes de foi et b) de faire respecter le privilège contre l'auto-incrimination[78]. Mais ni l'une ni l'autre de ces raisons ne s'appliquent aux preuves obtenues par écoute clandestine, peu importe comment elles ont été obtenues. Le fait que les déclarations soient dignes de foi, en particulier, est fonction de la fiabilité des

76. *R.* v. *Newall (No. 1)*, (1982) 67 C.C.C. (2d) 431, 136 D.L.R. (3d) 734 (C.S. C.-B.).

77. Voir *Malone* v. *Commissioner of Police of the Metropolis (No. 2)*, [1979] 2 All E.R. 620, 69 Cr. App. R. 168 (Ch.D.).

78. *Rothman* c. *La Reine*, [1981] 1 R.C.S. 640, p. 682-683; 59 C.C.C. (2d) 30, p. 63, le juge Lamer.

intercepteurs et non de la qualité du régime législatif qui les autorise à intercepter les communications. De plus, exception faite de la règle sur les confessions, au Canada, les éléments de preuve étaient admissibles avant l'adoption de la Charte, peu importe comment ils avaient été obtenus. Des tribunaux canadiens et d'autres cours de common law ont, sans le moindre scrupule, jugé recevables des éléments de preuve obtenus en violation d'une foule de droits garantis tant par le common law que par la loi, et même, en violation de la règle sur les confessions[79].

En matière de procédure régulière, le seul point sur lequel le Canada peut légitimement insister est que l'interception de communications privées à l'étranger n'ait pas été effectuée de mauvaise foi en vue de contourner les exigences canadiennes.

À ce propos, il serait utile de voir comment la question est réglée aux États-Unis où une grande partie des affaires jugées par les tribunaux portaient sur l'admissibilité de communications interceptées par les autorités canadiennes, tant avant qu'après l'adoption de la Partie IV.1 du *Code criminel*. À la lumière de ces décisions, il est évident que lorsque l'interception n'était pas illégale en vertu du droit canadien (même avant la promulgation de la Partie IV.1), les éléments de preuve étaient recevables devant les tribunaux américains qui ne sont pas visés par le «Title III»[80]. Cependant, l'unanimité n'est pas faite en ce qui concerne l'effet d'une interception illégale en vertu des lois canadiennes. Cela dépend, semble-t-il, du point de vue adopté par le tribunal saisi de la question. Dans l'affaire *United States* v. *Maher*[81], la Cour a tranché la question en appliquant le principe sous-tendant la règle d'exclusion américaine.

Dans l'arrêt *United States* v. *Phillips*[82], la Cour a abordé le problème de façon plus générale. Elle a jugé que le principe de la courtoisie entre les juges s'appliquait et elle a exclu la preuve obtenue par suite d'une interception illégale en vertu du droit canadien.

Selon le principe de base choisi, les deux approches sont défendables. La solution retenue dans l'affaire *Maher*, en particulier, laquelle exige que les règles américaines aient été respectées, semble convenir au contexte canadien. Un critère d'admissibilité qui repose sur le caractère choquant des éléments de preuve n'est pas sans rappeler le paragraphe 24(2) de la Charte. Il convient de noter que même en vertu du critère retenu dans l'affaire *Phillips*, il semblerait qu'il revienne à l'accusé de démontrer l'illégalité de l'interception en vertu du droit étranger[83].

Par conséquent, l'on pourrait résoudre le problème en veillant à ce que la Partie IV.1 ne s'applique à l'interception des communications à l'étranger que dans une très

79. *R.* v. *St. Lawrence*, (1949) 93 C.C.C. 376 (Haute cour Ont.).

80. *United States* v. *Cotroni*, 527 F.2d 708 (1975) (2d Cir.), demande rejetée 426 U.S. 906 (1975); *Stowe* v. *Devoy*, 588 F.2d 336 (1978) (2d Cir.), demande rejetée 442 U.S. 931 (1978).

81. *United States* v. *Maher*, 645 F.2d 708 (1981) (9th Cir.), p. 782-783.

82. *United States* v. *Phillips*, 479 F.Supp. 423 (1979), p. 437-438 (M.D. F.C.).

83. Dans l'affaire *Phillips*, cela n'a pas été difficile puisque l'action a été intentée à la suite de l'enquête menée sur les activités de Royal American Shows et qu'il y avait de la jurisprudence canadienne sur ce sujet précis.

petite mesure. Puisque l'interception a lieu à l'extérieur du Canada, comme nous l'avons expliqué ci-dessus, la protection du droit à la vie privée n'est pas un facteur déterminant. La nécessité de préserver l'intégrité du système lui-même l'emporte, comme l'a fait remarquer le juge Lamer en reconnaissant cette préoccupation dans l'arrêt *Rothman* c. *La Reine*[84] qui portait sur l'admissibilité d'une confession obtenue par supercherie.

De même, un manque d'égard criant pour la procédure suivie au Canada aux fins du contrôle de l'interception des communications privées ne devrait pas être encouragé. Dans l'affaire *Rothman*, le juge Lamer est d'avis que l'exclusion de la preuve est un bon moyen de contrôle lorsque, en raison de la conduite des personnes ayant autorité, admettre la preuve ternirait l'image de l'administration de la justice. Ce critère ressemble à la règle d'exclusion énoncée au paragraphe 24(2) de la *Charte canadienne des droits et libertés*, bien que le juge Lamer ait retenu un critère rigoureux exigeant que la conduite soit

> si indigne que la magistrature qui administre la justice criminelle soit justifiée de croire que, à moins de se dissocier de cette conduite en rejetant la déclaration, sa réputation et, par conséquent, celle de tout le système judiciaire, sera ternie[85].

Il semble peu probable qu'un critère aussi strict soit appliqué en vertu du paragraphe 24(2)[86] et nous avons songé à la possibilité de déterminer l'admissibilité de la preuve obtenue par l'interception de communications privées à l'étranger à l'aide du paragraphe 24(2) de la Charte. Mais cette solution pourrait faire naître une indésirable incertitude en droit car il n'est pas du tout certain que la conduite d'un représentant du gouvernement à l'étranger puisse porter atteinte aux droits d'une personne. Or, cette atteinte est une condition qui doit être remplie avant de pouvoir invoquer le paragraphe 24(2) de la Charte. Nous avons donc choisi une règle claire mais stricte, axée directement sur ce que nous considérons être un intérêt légitime du Canada, c'est-à-dire la protection de l'intégrité du système judiciaire.

Nous avons en outre décidé de faire porter sur l'accusé le fardeau de la preuve initial, qui une fois renversé fait entrer en jeu le fardeau de persuasion du ministère public. Cela aura pour effet, en pratique dans la plupart des cas, nous le reconnaissons, d'empêcher que soit faite une enquête sur la façon dont l'interception a été effectuée à l'étranger. Malheureusement, nous ne voyons pas d'autre solution.

Enfin, nous sommes d'avis que les interceptions effectuées à l'étranger devraient être assujetties au régime, du moins en ce qui concerne l'avis d'intention de produire une preuve.

---

84. *Supra*, note 78, p. 693-694 (R.C.S.), p. 72 (C.C.C.).
85. *Id.*, p. 696 (R.C.S.), p. 74 (C.C.C.).
86. Voir *R.* v. *Simmons*, (1984) 11 C.C.C. (3d) 193 (C.A. Ont.).

RECOMMANDATIONS

11. La preuve primaire et dérivée obtenue grâce à une interception faite hors du Canada, peu importe le lieu d'origine de la communication privée et que l'interception ait été effectuée légalement ou non, devrait être recevable pourvu que l'interception n'ait pas été faite dans un pays étranger en contravention des lois de celui-ci et avec la connivence des autorités canadiennes.

12. Le tribunal devant qui une communication privée interceptée à l'étranger est produite en preuve ne doit mener une enquête sur l'admissibilité de cette preuve que si la personne contre laquelle on tente de la faire admettre présente des éléments de preuve qui pourraient amener le tribunal à conclure que l'interception a été faite en contravention des lois du pays étranger avec la connivence des autorités canadiennes.

13. Les dispositions actuelles du paragraphe 178.16(4) devraient s'appliquer aux éléments de preuve obtenus grâce à des interceptions effectuées à l'étranger.

E. La surveillance participative : l'interception consensuelle

Une autre question qui se pose maintenant concerne l'interception consensuelle effectuée sans autorisation judiciaire parce que l'une des parties à la communication «privée» consent à ce qu'elle soit captée.

L'alinéa 178.11(2)*a*) soustrait les interceptions consensuelles du champ d'application de la loi. Deux situations sont visées : (1) l'un des interlocuteurs, à l'insu ou non de l'autre, enregistre lui-même les communications et (2) un tiers, avec le consentement de l'un des participants, intercepte et enregistre les communications. Compte tenu de la définition de l'expression «communication privée» dans l'arrêt *Goldman* c. *La Reine*[87], on peut conclure qu'il s'agit dans les deux cas de communications privées, du moins lorsque l'on tente de les produire en preuve contre la partie qui n'a pas donné son consentement à l'interception. Mais il convient de noter que dans ces deux cas, l'enregistrement et l'interception sont effectués légalement et que les éléments de preuve ainsi obtenus sont admissibles en vertu de l'alinéa 178.16(1)*a*). Aucune autorisation judiciaire préalable n'est nécessaire selon la loi.

La Cour suprême du Canada, dans l'arrêt *Goldman* c. *La Reine*, a jugé qu'un consentement visé par l'alinéa 178.11(2)*a*) est bon et valide «s'il s'agit de l'acte conscient de celui qui le donne et qui le fait pour des raisons qu'il considère suffisantes». Le consentement doit être «celui qu'il avait l'intention de donner et s'il le donne par suite de sa propre décision et sans être soumis à une coercition extérieure, le fait que ses

87. *Supra*, note 33.

motifs soient égoïstes et même répréhensibles selon certains critères ne l'invalide pas». En outre, le consentement ne doit pas avoir été obtenu par l'intimidation, par la force ni par des menaces d'employer la force de la part de la police. Cependant, on ne peut conclure à la coercition «simplement parce que le consentement est donné par suite de la promesse ou de l'espoir d'une indulgence ou d'une immunité de poursuites[88]».

Cet énoncé a fait l'objet de critiques dans le document de travail 30, du moins en ce qui concerne les fouilles, les perquisitions et les saisies[89]. Nous ne pensons pas toutefois que cette critique soit aussi justifiée lorsqu'il y a eu consentement à l'interception. Contrairement à la fouille ou à la perquisition faite avec le consentement de la personne visée, l'interception effectuée par suite du consentement d'une partie suppose, d'ordinaire, non seulement un consentement passif mais la participation active de cette personne.

La plupart du temps, lorsqu'il s'agit d'appliquer la loi, le consentement à l'interception donnera lieu à l'enregistrement d'une conversation entre le suspect et un policier ou un agent d'infiltration. Cependant, une foule d'autres contextes se prêtent à l'enregistrement d'une conversation avec le consentement d'un interlocuteur. Les hommes d'affaires, par exemple, peuvent enregistrer de façon routinière leurs propres conversations téléphoniques ou les propos tenus pendant leurs réunions. Une telle pratique n'est pas, d'ordinaire, considérée comme illégale.

Certaines préoccupations ont été exprimées à la Commission quant à l'opportunité de conserver le système actuel en vertu duquel les interceptions effectuées avec le consentement de l'une des parties sont soustraites au contrôle des autorités fédérales. Il se peut que cette façon de procéder soit beaucoup plus fréquente et persuasive, même dans les milieux officiels, que les autorisations judiciaires[90]. Les préoccupations exprimées concernent (1) l'intimité de la vie personnelle et (2) la preuve. En ce qui concerne l'intimité, on craint que l'usage répandu de l'enregistrement des communications par suite du consentement de l'un des interlocuteurs puisse, à la longue, gêner le libre échange des idées et nuire à la liberté de parole. Si les gens finissent par croire que leurs conversations sont enregistrées, ils risquent de s'autocensurer de peur qu'on ne leur reproche leurs propos.

En ce qui concerne la preuve, on s'inquiète surtout des risques de manipulation de la part de la personne qui sait que l'interception est effectuée. L'interlocuteur qui a donné son consentement peut orienter la conversation de façon à non seulement faire parler le suspect pour qu'il s'incrimine mais aussi à masquer sa propre participation et à fabriquer une preuve intéressée. En outre, la simple présentation de l'enregistrement peut induire en erreur le juge des faits qui ne sait pas dans quelles circonstances ces déclarations ont été faites.

---

88. *Id.*, p. 1005-1006 (R.C.S.), p. 24 (C.C.C.).

89. Document de travail sur les fouilles, les perquisitions et les saisies, *op. cit. supra*, note 47, p. 183-184.

90. J.G. Carr, «Electronic Surveillance By Consent under State Law» (novembre 1984), 11 *Search and Seizure Law Report* 77.

Deux solutions sont proposées en vue d'une réforme du droit. Premièrement, continuer de permettre l'interception consensuelle mais interdire la production en preuve de cet enregistrement. Deuxièmement, assujettir ce type d'interception au régime législatif et exiger l'obtention préalable d'une autorisation judiciaire. L'interception, même consensuelle, serait illégale autrement, et la preuve pourrait être exclue de la même façon que tout autre élément de preuve obtenu grâce à une interception illégale.

À notre avis, ni l'une ni l'autre de ces propositions ne sont acceptables. Pour l'essentiel, le droit actuel ne doit pas être modifié. Sur ce point, nous devons souligner l'influence exercée par la commission de réforme du droit de l'Australie. Bien qu'elle ait préconisé l'obtention obligatoire d'un mandat dans un document antérieur, elle a rejeté cette solution dans son rapport intitulé *Privacy*[91] et publié en 1983. Les raisons justifiant ce choix sont convaincantes et s'appliquent bien, sinon mieux, au Canada, compte tenu de la légalisation de l'interception avec consentement il y a dix ans. Voici l'opinion exprimée par la majorité des membres de la commission australienne :

> [TRADUCTION]
> 1131. *Les dangers de la réglementation de la surveillance participative*. La proposition voulant que la surveillance participative soit en général interdite comporte certains dangers. L'enregistrement des sons et des conversations est maintenant pratique courante entre amis ou à la maison, notamment à l'occasion d'événements, à l'insu de certains participants. Cela est fait pour s'amuser pendant les réceptions. Or, cette conduite ne devrait pas être sanctionnée par le droit pénal. Des conversations peuvent être enregistrées accidentellement au cours d'une réception. Le risque couru par la personne qui enregistre innocemment des événements sociaux pourrait être tout à fait disproportionné par rapport à l'acte répréhensible qu'on lui reproche.
>
> 1132. *Le problème fondamental n'est pas résolu*. La personne qui parle à une autre le fait à ses propres risques. Ses propos peuvent être recueillis et rapportés, plus ou moins fidèlement, par les autres parties à la conversation et à leur guise. La personne qui parle à une autre doit assumer le risque, d'ordinaire inhérent à cette situation, que son interlocuteur révélera ce qui lui a été confié. Il y a de nombreuses façons d'enregistrer une conversation. La prise de notes immédiatement après l'entretien en est une. La prise de notes en sténographie ou en écriture courante pendant la conversation en est une autre. Un dispositif d'écoute ne fait que remplacer les autres moyens d'enregistrement. Le problème fondamental demeure entier : la communication peut toujours être enregistrée ou rappelée dans des circonstances et à des fins échappant au contrôle de son auteur. La réglementation de certaines formes d'enregistrement n'aplanit pas cette difficulté[92].

Il ne semble pas opportun d'adopter la première proposition qui consiste à ne pas recevoir en preuve les conversations interceptées dans ce contexte. Il se peut fort bien que l'on ait recours à des témoignages d'experts pour expliquer les distorsions dues au fait que l'un des interlocuteurs sait qu'il y a interception. Ainsi, récemment des linguistes ont été cités dans plusieurs procès en vue de réduire l'importance attachée par le juge

91. Law Reform Commission of Australia, *Privacy* [Report No. 22], Canberra, Australian Government Publishing Service, 1983, 2 vol.

92. *Id.*, vol. 1, art. 1131-1132, p. 49.

des faits à une confession[93]. Mais, à notre avis, il serait mal avisé d'exclure en règle générale des éléments de preuve qui risquent d'être très pertinents et très utiles au juge des faits. Pour en être convaincu, il suffit de considérer les problèmes suivants : l'avocat de la défense pourrait-il contre-interroger un témoin (disons un indicateur) au sujet de la transcription d'une conversation enregistrée afin de mettre en doute sa faculté de se rappeler cette conversation? L'accusé serait-il empêché de produire l'enregistrement magnétique d'une communication faite à une autre personne et susceptible de faire naître un doute sur sa propre culpabilité? Si l'accusé nie que la conversation a eu lieu comme le prétend le policier, sera-t-il impossible au ministère public de produire un enregistrement de cette conversation? Nous estimons qu'une réglementation des interceptions de consentement compliquerait inutilement les choses, sans pour autant assurer une meilleure appréciation des faits ni mieux protéger l'intimité de la vie privée dont le respect est revendiqué à bon droit.

Il convient de remarquer qu'en raison de la modification proposée de la définition de l'expression «communication privée», il sera nécessaire d'allonger la liste des exemptions à l'infraction prévue au paragraphe 178.18(1). Celui-ci dispose que quiconque possède un dispositif, sachant que sa conception le rend principalement utile à «l'interception clandestine de communications privées» est coupable d'un acte criminel. Selon la formulation énoncée dans l'affaire *Goldman*[94], on ne peut savoir avec certitude si la communication enregistrée par une partie constitue une communication privée qu'après le fait accompli puisque pour déterminer cette question il faut savoir qui est l'auteur de la communication.

Nous proposons plutôt que, même si une partie à la conversation donne son consentement à l'enregistrement ou procède dans les faits à l'enregistrement elle-même, la communication soit privée si l'autre partie pouvait raisonnablement s'attendre à ce qu'elle ne soit pas interceptée. Par voie de conséquence, la personne qui possède un enregistreur capable d'enregistrer ses propres conversations à l'insu de ses interlocuteurs pourra être poursuivie au criminel, selon le sens donné au mot «clandestine». Il faut donc modifier l'article 178.11 afin qu'une interception effectuée dans ces conditions ne soit pas illégale. La modification de l'article 178.18 par l'article 25 du projet de loi C-18 ne serait plus nécessaire[95].

RECOMMANDATIONS

14. Il devrait continuer d'être prévu à l'article 178.11 qu'il n'est pas illégal d'intercepter une communication privée avec le consentement exprès ou tacite d'une personne qui y participe.

---

93. Voir *R.* v. *Lapointe and Sicotte*, (1983) 9 C.C.C. (3d) 366 (C.A. Ont.); *R.* v. *Lessard*, (1982) 10 C.C.C. (3d) 61 (C.A. Qué.).

94. *Supra*, note 33.

95. Cette modification ajoute à la liste des exemptions de l'alinéa 178.18(2)*b*.1) la disposition qui suit :
à une personne en possession d'un dispositif, d'un élément ou d'une pièce d'un dispositif, sous la direction d'un officier de police ou d'un agent de police, afin de l'aider dans l'exercice de ses fonctions;

15. L'infraction prévue au paragraphe 178.18(1) ne devrait pouvoir être reprochée à une personne en possession d'un dispositif, ou d'un élément de celui-ci, qu'elle utilise ou entend utiliser en vue de procéder à une interception avec le consentement d'une des personnes qui participe à la communication privée.

16. (1) Avant de procéder à l'interception visée par le présent article, le policier devrait informer la personne dont on cherche à obtenir le consentement, de son droit de refuser son consentement et de le retirer en tout temps.

(2) Le consentement visé par le présent article peut être donné soit oralement, soit par écrit.

17. La signature d'une personne sur un document l'informant de son droit de refuser son consentement et de le retirer en tout temps ou l'enregistrement d'un tel consentement constitue une preuve *prima facie* du consentement donné par la personne à l'interception.

II. L'autorisation

A. La demande d'autorisation

Aux termes de l'article 178.12 du *Code criminel*, la demande d'autorisation doit être présentée *ex parte* par un mandataire désigné à cette fin à un juge d'une cour supérieure de juridiction criminelle ou à un juge défini à l'article 482, ce qui comprend un juge de cour de comté ou de district dans certaines provinces et un juge de la Cour provinciale au Québec. La présentation *ex parte* d'une telle demande, c'est-à-dire en la seule présence du juge, du mandataire et du policier auteur de l'affidavit qui doit accompagner la demande conformément au paragraphe 178.12(1), suscite certaines préoccupations. Bien que la procédure à suivre pour obtenir un mandat de perquisition ordinaire puisse inspirer des craintes similaires, la Cour suprême du Canada a décidé qu'une telle demande pouvait être présentée à huis clos[96].

Évidemment, ce serait faire échec à l'objet de la demande que de notifier la personne visée. Quoi qu'il en soit, on a proposé qu'un intervenant (*amicus curiae* ou *amicus publicae*) soit en quelque sorte chargé de représenter les intérêts de cette personne et présumément ceux de la société dans une certaine mesure. Cohen a fait remarquer que [TRADUCTION] «la confidentialité serait préservée et le public recevrait une nouvelle fois l'assurance que le respect de la vie privée n'est pas un vain mot[97]». L'idée d'une telle

96. *Le procureur général de la Nouvelle-Écosse* c. *MacIntyre*, [1982] 1 R.C.S. 175, 65 C.C.C. (2d) 129.

97. S.A. Cohen, *Invasion of Privacy : Police and Electronic Surveillance in Canada*, Toronto, Carswell, 1983, p. 137.

intervention n'a pas été reprise et bien que les préoccupations soulevées par Cohen et par d'autres ne puissent être facilement écartées, nous ne sommes pas disposés à recommander l'instauration d'un tel régime si nos propositions relatives à la divulgation des documents utilisés lors de la demande sont retenues. Compte tenu du fait qu'en définitive, cet intervenant serait informé par les autorités, il n'est pas évident qu'un tel régime garantisse véritablement l'intimité de la vie privée. Nous craindrions que cet intervenant ne donne simplement l'illusion que le droit à la vie privée est protégé et que sa présence n'affaiblisse les arguments avancés en faveur de l'adoption des recommandations relatives à la divulgation des faits qui, à notre avis, pourrait offrir une protection véritable et permettre l'instauration d'un régime fondé sur la responsabilité.

À l'heure actuelle, l'audition *ex parte* se déroule à huis clos et son contenu n'est pas consigné. Il n'y a pas de sténographe judiciaire et aucun enregistrement n'est fait. Il n'est pas certain que le juge puisse interroger l'auteur de l'affidavit pour suppléer les faits invoqués dans ce document. L'on n'a pas manqué de faire remarquer qu'au moment du renouvellement de l'autorisation, outre la demande écrite et l'affidavit, l'on pouvait étayer la demande par «les autres renseignements que le juge peut exiger». À nouveau, on ne sait pas exactement comment doivent être présentés ces renseignements. Cette incertitude peut avoir de graves conséquences si les recommandations relatives à la divulgation sont adoptées car la procédure à suivre pour obtenir une autorisation sera plus ouverte et donc, plus facile à contester. Bien que les juges saisis d'une demande d'autorisation doivent être encouragés à mettre en doute les faits invoqués dans l'affidavit, les déclarations faites par le policier et sur lesquelles le juge se fonde pour accorder l'autorisation doivent être consignées afin qu'elles puissent être examinées plus tard. Par conséquent, nous sommes en faveur de la procédure recommandée dans le document de travail 30 concernant les fouilles, les perquisitions et les saisies[98].

RECOMMANDATION

18. La demande d'autorisation ou de renouvellement devrait continuer d'être présentée par écrit et d'être accompagnée par un affidavit rédigé par un policier. L'audition devrait se dérouler *ex parte* et à huis clos. Le juge devrait être habilité à assermenter le policier pour vérifier les faits supplémentaires sur lesquels s'appuie la demande. Cependant, si le juge se fonde sur de tels faits pour décider de la demande, ces faits seront consignés et placés dans un paquet scellé.

B. Les motifs de l'autorisation

Les motifs permettant au juge d'accorder l'autorisation sont énoncés au paragraphe 178.13(1). Celui-ci vise à faire ressortir la nature extraordinaire de l'intrusion. L'essentiel de ces motifs est contenu à l'alinéa *b*), lequel exige que le juge soit convaincu

98. Document de travail sur les fouilles, les perquisitions et les saisies, *op cit. supra*, note 47, p. 209-212.

que d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête.

Si cette exigence respecte, dans une certaine mesure, le critère du «dernier recours» qui conditionne à bon droit l'utilisation de cette méthode d'investigation, elle ne règle pas le problème plus nébuleux de la gravité de l'infraction présumée. Comme nous l'avons indiqué ci-dessus, bien que la surveillance électronique soit considérée comme un outil nécessaire à la lutte contre les activités du crime organisé et les autres crimes graves, en pratique, son utilisation n'a jamais été aussi restreinte. Au cours des consultations que nous avons tenues, certains craignaient que la surveillance électronique ne soit à tort utilisée aux fins d'enquête sur des infractions de moindre importance. Même si nous n'avons pas réduit considérablement la liste des infractions que peut viser une autorisation à l'article 178.1, nous estimons toujours que l'intérêt public est mieux servi par la restriction de l'utilisation de ce moyen d'investigation si attentatoire aux cas graves d'infractions qui peuvent faire l'objet d'une autorisation. Par conséquent, nous proposons qu'une modification soit apportée à l'alinéa 178.13(1)*a*), lequel dispose actuellement que le juge doit être convaincu «que l'octroi de cette autorisation servirait au mieux l'administration de la justice ...».

RECOMMANDATION

19. L'alinéa 178.13(1)*a*) devrait être modifié. Il devrait disposer que le juge peut accorder une autorisation lorsqu'il est convaincu que cela servirait au mieux les intérêts de l'administration de la justice et l'intérêt public, compte tenu de la gravité de l'infraction qui fait l'objet de l'enquête.

C. Les infractions interprovinciales

Les bandes organisées de criminels et les autres types de criminels ne respectent pas nécessairement les frontières provinciales. La question de savoir si les juges d'une province avaient compétence pour autoriser une interception dans une autre province a été soulevée. Jusqu'ici, la réponse semble être négative[99], bien que dans l'arrêt *R.* v. *Bengert*[100], le juge Berger ait décidé que la Cour supérieure pouvait autoriser l'interception de communications privées à l'extérieur de la province. À notre avis, à l'heure actuelle, la Partie IV.1 ne le permet pas. Du reste, comme l'a fait remarquer le juge Osler dans l'affaire *Re Application for Authorization to Intercept Private Communications*, [TRADUCTION] «l'objet de l'autorisation et les conditions auxquelles elle est assujettie peuvent varier considérablement d'une province à l'autre[101]».

99. *Supra*, note 76, le juge Bouck. Voir aussi *Re Application for Authorization to Intercept Private Communications*, (1983) 9 C.C.C. (3d) 347 (Haute cour Ont.), le juge Osler.

100. *R.* v. *Bengert*, [1979] 1 W.W.R. 193 (C.S. C.-B.).

101. *Supra*, note 99, p. 349.

Plusieurs solutions ont été proposées pour résoudre ce problème :

a) Un système de confirmation semblable à la procédure prévue au paragraphe 443(2) du *Code criminel* :

Bien que cette solution ait rallié les suffrages de plusieurs représentants du gouvernement, nous pensons qu'elle soulève de graves problèmes. Par exemple, sur quels renseignements se fonderait le juge effectuant le contrôle? Devrait-il vérifier la demande initiale, ou se contenter d'approuver l'autorisation? Quels critères régiraient l'exercice de son pouvoir discrétionnaire? Qu'en serait-il de la police? Si l'autorisation est confirmée, serait-elle obligée d'appliquer l'ordonnance et peut-être d'affecter des ressources déjà insuffisantes à un projet auquel elle n'aurait normalement pas accordé la priorité? Il faudrait au moins que la demande de confirmation de l'autorisation soit accompagnée d'un affidavit rédigé par un policier du ressort du juge, indiquant une volonté d'appliquer l'ordonnance et indiquant que la demande a été approuvée par un mandataire du procureur général de la province ou du solliciteur général, selon le cas.

b) Une modification à l'article 178.13 permettant au juge d'autoriser une interception dans une autre province :

Nous pensons que les questions soulevées par le juge Osler auxquelles nous avons fait allusion ci-dessus sont pertinentes et que cette solution n'est pas bonne.

c) Une modification à l'article 178.13 permettant à un juge de la Cour fédérale d'autoriser l'interception de communications privées partout au Canada :

Aucune des personnes consultées n'a retenu cette solution. Mis à part toute autre considération, les juges de la Cour fédérale n'ont jamais auparavant connu des demandes d'autorisation de surveillance électronique en vertu de la Partie IV.1 et n'ont pas d'expérience dans ce domaine. Leur action en matière pénale est en général plutôt limitée et il serait peut-être injuste d'exiger qu'ils statuent sur ces demandes interprovinciales.

d) Le statu quo :

Pour l'essentiel, il vaut mieux à notre avis laisser les choses comme elles sont, sous réserve de la modification examinée ci-dessous. Selon les divers organismes chargés de l'application de la loi, il ne s'agit pas d'un problème grave. Grâce à la collaboration des autres forces de police, ils ne se heurtent à aucune difficulté grave.

Cependant, l'un des problèmes qui nous a été soumis justifie à notre avis une réforme. Il est imputable au libellé des alinéas 178.12(1)*a*) et *b*) dont voici la teneur :

> **178.12** (1) Une demande d'autorisation doit être présentée *ex parte* et par écrit à un juge d'une cour supérieure de juridiction criminelle, ou à un juge défini à l'article 482, et être signée par le procureur général de la province où la demande est présentée ou par le solliciteur général du Canada ou par un mandataire spécialement désigné par écrit aux fins du présent article par

> *a*) le solliciteur général du Canada lui-même, si l'infraction faisant l'objet de l'enquête est une infraction pour laquelle des poursuites peuvent, le cas échéant, être engagées sur l'instance du gouvernement du Canada et conduites par le procureur général du Canada ou en son nom, ou
>
> *b*) le procureur général d'une province lui-même, pour toute autre infraction se situant dans cette province, ...

Aux termes de ces dispositions, il semble qu'un juge ne serait pas habilité à autoriser une demande lorsque l'infraction n'est pas commise ou n'a pas été commise dans la province. Lorsqu'une infraction est commise dans une province et qu'il y a lieu de croire que les suspects vivent dans une autre province, il semble que ni l'une ni l'autre des provinces ne puisse demander une autorisation. Il s'agit certainement d'un oubli. La loi devrait être modifiée afin de permettre aux autorités d'une province de demander une autorisation, même si l'infraction a été commise dans une autre province. En outre, une telle modification serait tout à fait compatible avec nos vues car nous estimons que l'autorisation devrait être principalement axée sur la personne.

RECOMMANDATION

20. Le paragraphe 178.12(1) devrait être modifié afin qu'une autorisation puisse être accordée lorsque les communications de la personne visée peuvent être interceptées dans la province, même s'il est allégué que l'infraction a été commise dans une autre province.

D. La restriction des interceptions

Bien que le respect de la vie privée et le principe de la modération doivent être considérés comme des facteurs importants, sinon comme des principes déterminants, en ce qui a trait à l'exercice de moyens d'enquête aussi attentatoires que la surveillance électronique, ils retiennent peu l'attention une fois que l'ordonnance est accordée. C'est pourquoi la restriction des interceptions figure parmi les questions les plus épineuses que suscite l'examen de l'actuelle législation. Il s'agit de n'intercepter et de n'enregistrer que les communications se rapportant à l'enquête. Contrairement à la législation fédérale américaine, la Partie IV.1 du *Code criminel* n'est guère explicite sur ce point. L'autorisation désignera certaines personnes, comportera certaines adresses et, peut-être, certains numéros de téléphone. Elle contiendra aussi une clause générale permettant l'interception des communications faites par les tiers qui sont en rapport avec les personnes nommées dans l'autorisation. Les lignes téléphoniques ne seront d'ordinaire surveillées que pendant deux ou trois périodes de huit heures. Mais qu'ils soient surveillés ou non, les dispositifs d'enregistrement fonctionnent automatiquement et consignent tous les appels provenant de ce poste ou acheminés vers lui. En outre, pendant la surveillance, un bref résumé des communications faites au cours de chaque appel est inscrit dans un procès-verbal où les appels sans intérêt pour l'enquête sont souvent désignés comme tels.

Certaines formes d'écoute font l'objet d'une surveillance plus étroite. Mais même lorsqu'une surveillance humaine du dispositif d'enregistrement est assurée, aucune directive n'exige que les communications inutiles ne soient pas enregistrées.

Dans les faits, l'autorisation agit à la manière d'un énorme aspirateur électronique qui avale sans discrimination les communications pertinentes et celles qui ne le sont pas. Les représentants du gouvernement et de la police nous ont fait valoir que des dispositions tendant à restreindre l'enregistrement des communications, selon leur intérêt pour l'enquête, enlèveraient toute efficacité à l'écoute clandestine comme méthode d'investigation. Ils ont souligné l'utilisation relativement peu fréquente de l'écoute clandestine aux États-Unis, état de choses qu'ils attribuent aux dispositions strictes concernant la limitation des enregistrements, lesquelles font de l'écoute clandestine un moyen d'investigation coûteux et peu efficace. Nous ne sommes pas convaincus du bien-fondé de ces affirmations, compte tenu de la jurisprudence examinée ci-dessous, mais il est utile de rappeler que la législation relative à l'écoute clandestine visait à en faire un outil de dernier recours en raison de ses graves répercussions sur l'intimité de la vie privée et la liberté. Il n'est pas évident en soi que la loi doive être rédigée de manière à privilégier l'écoute clandestine comme méthode d'investigation.

La jurisprudence récente tend à favoriser la disparition des rares garanties en matière de restriction des interceptions contenues dans la législation actuelle. Dans l'affaire *R. v. Samson (No. 6)*[102], par exemple, la Cour a jugé qu'il était tout à fait licite d'intercepter, en vertu d'une autorisation ordinaire, les appels des marchands et autres utilisateurs occasionnels du poste de téléphone faisant l'objet d'une surveillance car leurs appels pouvaient contenir des messages à l'intention des personnes visées par l'autorisation ou d'autres renseignements de nature à faire avancer l'enquête. À notre connaissance, sauf de très rares cas d'exception (interception des appels d'un juge ou d'un avocat), les seules dispositions relatives à la restriction des enregistrements figurant dans la plupart des autorisations portent que l'interception des appels originant d'un téléphone public ne peut être effectuée que si une surveillance visuelle est assurée en même temps. Il ne s'agit pas nécessairement d'une condition prévue par la législation actuelle, mais les mandataires la font figurer «volontairement» dans l'autorisation. Il se peut que les juges refuseraient autrement d'autoriser l'interception des communications privées faites dans un téléphone public, c'est-à-dire si l'autorisation le permettait. (Il convient de souligner qu'une clause courante dans la plupart des autorisations permet l'interception des communications faite en tout lieu, fixé à demeure ou mobile, que la personne désignée peut fréquenter.)

Il faut également faire remarquer que la Charte peut avoir d'importantes incidences dans ce domaine. Ajoutons que les obligations du Canada, à titre de signataire du *Pacte international relatif aux droits civils et politiques* des Nations Unies, ne doivent pas

102. *R. v. Samson (No. 6)*, (1982) 37 O.R. (2d) 48, 237 (Cour de comté Ont.), infirmé *supra*, note 58.

être prises à la légère[103]. Le respect de l'intimité de la vie privée et l'obligation de protéger les citoyens contre toute atteinte arbitraire et abusive sont inscrits en filigrane dans ces documents. On peut se demander s'il est arbitraire et abusif de sanctionner un système permettant l'interception et l'enregistrement de tous les appels téléphoniques effectués à l'aide d'un poste déterminé, sans égard à l'identité de l'utilisateur ni au contenu de la conversation.

À notre avis, la condition essentielle à l'adoption d'une disposition appropriée en matière de restriction des enregistrements est la reconnaissance du droit à la vie privée. L'interception ne devrait être autorisée que s'il y a des motifs de croire que la personne visée par l'autorisation participe à l'activité criminelle désignée. Il serait incompatible avec les dispositions de la Charte, avec nos obligations à titre de signataire du *Pacte international relatif aux droits civils et politiques* et avec les principes qui devraient guider la procédure pénale de permettre une immixtion généralisée dans l'intimité d'autres personnes sous le prétexte spécieux que de telles interceptions peuvent faire avancer une enquête. En revanche, il n'est pas nécessairement injuste de permettre l'interception et l'enregistrement de tous les appels de la personne désignée même si certains, sinon la majorité, de ces appels ne sont peut-être pas pertinents. Exiger que seuls les appels pertinents soient interceptés et enregistrés peut avoir d'importantes répercussions sur le droit de l'accusé à une défense pleine et entière. La production de la seule partie pertinente d'une conversation, c'est-à-dire des paroles incriminantes, peut lui être préjudiciable et induire en erreur le juge des faits. Un appel pris hors contexte peut être interprété de façon très différente. En plus, cette façon de procéder se révèle une tâche quasiment impossible à accomplir pour la personne chargée de la surveillance, car elle doit pouvoir prévoir quand la conversation portera sur l'activité illégale.

Il faudrait que le dispositif d'enregistrement fasse l'objet d'une surveillance humaine constante pour assurer véritablement une restriction efficace de l'enregistrement des communications. Bien que les avis soient partagés sur ce sujet, il est probablement exact de dire que cette mesure triplerait, au moins, les frais entraînés par l'enquête. Par conséquent, il faut soigneusement apprécier les avantages qu'elle représente pour l'intimité de la vie privée. En définitive, nous ne sommes pas convaincus qu'il vaille la peine d'assurer une surveillance constante, eu égard aux avantages minimes que comporterait cette mesure par rapport à l'augmentation considérable des coûts qu'elle entraînerait. Pour mieux illustrer notre propos, nous examinerons ci-après la situation aux États-Unis.

---

103. Le Canada a adhéré au *Pacte international relatif aux droits civils et politiques* des Nations Unies qui est entré en vigueur le 23 mars 1976. Voici le paragraphe 17(1) de ce document :

> Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

L'article 8 (fouilles, perquisitions ou saisies abusives) et l'article 7 (protection de la vie, liberté et sécurité de la personne) de la Charte reconnaissent le respect de la vie privée comme l'un des attributs fondamentaux de la société moderne. Certes, il reste à voir si l'article 7 en particulier sera interprété de façon à garantir un droit général à l'intimité de la vie privée dont le respect pourrait être assuré par l'entremise des tribunaux à l'instar des cinquième et quatorzième amendements des États-Unis qui protègent la «liberté» par la règle de l'application régulière de la loi. Voir L. Tribe, *American Constitutional Law*, New York, Foundation Press, 1978, en particulier le chapitre 15 intitulé «Rights of Privacy and Personhood» et les commentaires du juge d'appel Parker dans l'arrêt *R.* v. *Morgentaler, Smoling and Scott*, (1984) 14 C.C.C. (3d) 258, p. 299-314 (Haute cour Ont.).

L'arrêt *Scott* v. *United States*[104] fait autorité en la matière aux États-Unis. Aux termes du paragraphe 2518(5) du Title III[105], l'ordonnance doit comporter une clause prévoyant que l'interception [TRADUCTION] «doit être réalisée de manière à réduire au minimum l'interception des communications qui ne sont pas par ailleurs susceptibles de faire l'objet d'une interception en vertu du présent chapitre». Bien que dans cette affaire, l'ordonnance ait contenu une telle clause, les policiers ont intercepté *tous* les appels, dont seulement 40 pour cent étaient liés à l'infraction visée (trafic de stupéfiants). La majorité des juges a cependant décidé que les exigences du Title III n'avaient pas été transgressées. La Cour a adopté une norme de modération objective plutôt qu'une norme fondée sur l'appréciation des motifs de la police ou de sa bonne foi[106].

Si, comme dans l'affaire *Scott*, l'interception de *tous* les appels était légale, même en vertu d'un régime exigeant qu'une surveillance humaine du dispositif d'enregistrement soit assurée et que seuls les appels pertinents soient enregistrés, on voit mal les avantages que représentent ces garanties en ce qui concerne le droit à la vie privée. En outre, quelle que soit la méthode choisie pour restreindre l'enregistrement des appels, il y a tout de même immixtion dans la vie privée, ne serait-ce que par le surveillant. Le seul avantage serait peut-être que les conversations ne sont pas enregistrées et qu'il ne subsiste pas de dossier permanent. Nous estimons que l'adoption d'une disposition législative rendant obligatoire la limitation de l'enregistrement des communications et la surveillance du dispositif d'enregistrement n'est pas justifiée. En revanche, nos experts-conseils étaient tous d'avis qu'une liste de conditions relatives à cette limitation serait utile. Le juge autorisant l'interception pourrait les ajouter à l'ordonnance, tout comme il le fait dans une ordonnance de probation à l'aide du paragraphe 663(2) du *Code criminel* qui comporte une liste de conditions précises dont peut se servir le juge. Selon nous, cette solution réglerait de façon pratique un problème très épineux.

Les communications entre l'avocat et son client ainsi que les autres communications protégées représentent un aspect particulier du problème de la limitation de l'enregistrement des communications. Suite à la mise sous écoute du téléphone privé situé dans le salon des avocats au Palais de justice de Sault Ste-Marie, les paragraphes 178.13 (1.1) et (1.2) ont été ajoutés au *Code criminel*. En voici la teneur :

> (1.1) Le juge auquel est faite une demande d'autorisation en vue d'intercepter des communications privées au bureau ou à la résidence d'un avocat, ou à tout autre endroit qui sert ordinairement à l'avocat ou à d'autres avocats pour la tenue de consultations avec des clients, doit refuser de l'accorder à moins qu'il ne soit convaincu qu'il existe des motifs raisonnables de croire que l'avocat, un autre avocat qui exerce le droit avec lui, un de ses employés, un employé de cet autre avocat ou une personne qui habite sa résidence est partie à l'infraction ou s'apprête à le devenir.
>
> (1.2) Le juge qui accorde l'autorisation d'intercepter des communications privées à un endroit décrit au paragraphe (1.1) doit y inclure les modalités qu'il estime opportunes pour protéger les communications sous le sceau du secret professionnel entre l'avocat et son client.

104. *Scott* v. *United States*, 436 U.S. 128 (1978).

105. Title III, *supra*, note 67, n° 802, 82 *Stat.* 212.

106. *Supra*, note 104, p. 139-141.

Toutefois, dans le récent arrêt *R.* v. *Chambers*[107], il a été décidé que le paragraphe 178.13(1.2) n'obligeait pas le juge à imposer des conditions en vue de protéger les communications faites sous le sceau du secret professionnel. Néanmoins, le juge d'appel Anderson a estimé que [TRADUCTION] «dans la plupart des cas ... une disposition devrait être insérée dans l'autorisation en vue de protéger les personnes autres que celles qui y sont désignées[108]».

À notre avis, le législateur entendait par l'adoption des paragraphes 178.13 (1.1) et (1.2) restreindre l'interception des communications protégées. Dans ces conditions, des modalités doivent obligatoirement être insérées à cette fin.

Sur ce point, il faut examiner le problème soulevé par l'interception des communications faites entre l'avocat et son client par suite de l'interception des appels du client. Il y a, à cet égard, un rapport d'analogie avec le droit relatif aux fouilles, aux perquisitions et aux saisies. Dans l'arrêt *Descôteaux* c. *Mierzwinski*[109], la Cour a jugé que le privilège protégeant les communications entre l'avocat et son client ne constituait pas une simple règle de preuve. La portée de ce privilège est beaucoup plus grande et, en fait, ce droit à la confidentialité a donné naissance à une règle de fond.

D'après la règle formulée par le juge Lamer, la confidentialité des communications entre client et avocat peut être soulevée en toutes circonstances où ces communications seraient susceptibles d'être dévoilées sans le consentement du client[110].

Certes, en ce qui concerne l'admissibilité de la preuve, toute la vigueur du privilège protégeant ces communications est préservée par le paragraphe 178.16(5), mais à nos yeux, la règle de fond énoncée par le juge Lamer a des incidences sur l'interception que devrait reconnaître le législateur. Il convient de noter que dans le récent arrêt *R.* v. *Heikel*[111], rendu par la Cour du Banc de la Reine de l'Alberta, le juge Wachowich a exclu tous les éléments de preuve obtenus à l'aide de l'écoute clandestine en raison de l'interception et de l'enregistrement répétés des communications faites entre l'avocat et son client après que le prévenu eut été accusé pour la première fois, en dépit du fait que le ministère public n'ait pas eu l'intention de produire aucune de ces conversations en preuve. Le juge s'est également élevé contre l'interception et l'enregistrement répétés des conversations faites entre les deux accusés qui étaient mari et femme, bien que de telles communications soient aussi protégées. Cependant, comme le privilège protégeant les communications entre époux concerne uniquement la preuve et ne constitue pas, semble-t-il, une règle de fond[112], nous ne recommandons pas la restriction obligatoire de l'enregistrement de telles communications.

---

107. *R.* v. *Chambers*, (1983) 9 C.C.C. (3d) 132 (C.A. C.-B.)

108. *Id.*, p. 141.

109. *Descôteaux* c. *Mierzwinski*, [1982] 1 R.C.S. 860, 70 C.C.C. (2d) 385; voir les motifs du juge Lamer.

110. *Id.*, p. 875 (R.C.S.), p. 400 (C.C.C.).

111. *R.* v. *Heikel*, B.R. de l'Alberta, 25 mai 1984 (le juge Wachowich), jugement inédit.

112. Voir *Rumping* v. *Director of Public Prosecutions*, [1962] 3 All E.R. 256 (H.L.) et *R.* v. *Kotapski*, (1984) 13 C.C.C. (3d) 185 (C.A. Qué.).

Le lecteur remarquera que nous n'avons pas abordé les conséquences d'un manquement aux modalités destinées à assurer le respect des exigences relatives à la limitation des enregistrements imposées par le juge. Ce problème s'est avéré très difficile à résoudre aux États-Unis (voir à titre d'illustration les arrêts *United States* v. *Dorfman*[113] et *United States* v. *Suquet*[114]). Étant donné que nous recommandons que soit retenue la règle d'admissibilité énoncée à l'actuel article 178.16, nous ne voyons pas pourquoi il faudrait rédiger des règles d'admissibilité spéciales lorsque des modalités relatives à la limitation des enregistrements ont été insérées dans l'autorisation. Il appartiendra au juge de déterminer lors du procès si, dans chaque cas particulier, l'interception respectait les modalités de l'autorisation et était par conséquent légale.

RECOMMANDATIONS

21. L'autorisation ne devrait être accordée qu'à l'égard des personnes dont l'interception des communications privées fera avancer l'enquête sur l'infraction, du fait de leur participation à cette infraction.

22. L'article 178.13 devrait être modifié afin que le juge puisse insérer dans l'autorisation les modalités suivantes :

a) le dispositif devrait faire l'objet d'une surveillance humaine constante pendant toute la période où l'on se propose d'intercepter ou d'enregistrer des communications privées;

b) dans toute la mesure raisonnablement possible, seules les conversations des personnes visées devraient être interceptées et enregistrées;

c) lorsque l'on se propose d'intercepter les communications à un téléphone que le public peut utiliser, l'interception devrait faire l'objet d'une surveillance humaine et être accompagnée d'une surveillance visuelle;

d) il convient de prendre des mesures raisonnables pour éviter l'interception de communications privées entre conjoints, entre les médecins et leurs patients ou des autres communications faites sous le sceau du secret professionnel;

e) il convient de prendre des mesures raisonnables pour éviter d'intercepter les communications privées des personnes visées lorsque, d'après les communications antérieures, elles ne peuvent vraisemblablement pas faire avancer l'enquête sur l'infraction;

f) l'interception devrait cesser lorsque le but de l'enquête a été atteint;

g) l'interception d'une ligne téléphonique utilisée par plusieurs personnes ne doit être réalisée que lorsque la ligne fait l'objet d'une surveillance;

h) toute autre modalité que le juge estime opportune afin de restreindre l'interception et l'enregistrement des communications privées n'ayant aucun rapport avec l'enquête.

---

113. *United States* v. *Dorfman*, 542 F.Supp. 345 (1982), N.D. Ill., appel rejeté, 690 F.2d 1217.

114. *United States* v. *Suquet*, 547 F.Supp. 1034 (1982).

23. L'autorisation devrait porter, comme condition, que lorsqu'on se propose d'effectuer une interception dans un lieu mentionné au paragraphe 178.13(1.1), il convient de prendre des mesures raisonnables afin de veiller à ce que les communications entre avocats et clients, protégées par le secret professionnel, ne soient ni interceptées ni enregistrées.

24. Lorsqu'il y a lieu de croire que si l'autorisation est accordée, les communications entre la personne visée et son avocat, protégées par le secret professionnel, risquent d'être interceptées, ce fait devrait être divulgué au moment où la demande d'autorisation est présentée.

25. Dans les cas où la recommandation 21 s'applique, l'autorisation devra porter, comme condition, que dans la mesure raisonnablement possible, les communications entre la personne visée et son avocat, protégées par le secret professionnel, ne doivent être ni interceptées ni enregistrées.

E. Les clauses générales

Grâce à l'arrêt *R.* v. *Welsh and Iannuzzi (No. 6)*[115], les conséquences du défaut de prévoir l'interception des communications de personnes non désignées dans l'autorisation sont devenues évidentes : les conversations n'ont pas été admises au motif que l'interception n'avait pas été effectuée légalement. Depuis, toutes les autorisations comportent une clause générale permettant l'interception des communications faites par des inconnus. Il convient de faire remarquer que cette clause n'est requise que lorsque ni l'un ni l'autre des interlocuteurs ne sont mentionnés dans l'autorisation. Si au moins l'un d'entre eux est désigné, l'interception est autorisée et légale, sauf si l'identité de l'un des correspondants est tenue secrète de mauvaise foi[116].

Le libellé de ces clauses varie beaucoup, mais elles visent toutes à résoudre le problème posé par la production des communications interceptées entre des personnes non désignées dans l'autorisation. Le principal point en litige est la détermination de la portée de la clause générale. Il est souvent allégué que l'accusé était connu de la police au moment où l'autorisation a été obtenue et que, par conséquent, l'interception de ses appels n'est pas autorisée par une clause visant les «inconnus». Or, il nous semble que ce débat a peu d'incidence sur la protection de la vie privée. C'est également l'avis exprimé par la Cour suprême des États-Unis dans l'affaire *Donovan*[117].

En ce qui concerne l'intimité de la vie privée, la question est de savoir dans quelle mesure la loi devrait permettre l'interception des communications faites par des personnes qui ne sont pas liées à l'infraction au moment où l'autorisation est obtenue. Le

115. *Supra*, note 31.

116. *R.* v. *Gill*, (1980) 56 C.C.C. (2d) 169 (C.A. C.-B.).

117. *United States* v. *Donovan*, 429 U.S. 413 (1977).

problème découle aussi de la condition préliminaire à laquelle est assujettie l'interception des communications d'une personne déterminée, à savoir qu'il doit s'agir d'une personne «dont les communications privées devraient être interceptées du fait qu'on a des motifs raisonnables et probables de croire que cette interception pourra être utile à l'enquête relative à l'infraction[118]».

Si la surveillance électronique est considérée comme une fouille, une perquisition ou une saisie au sens de l'article 8 de la *Charte canadienne des droits et libertés*, une loi autorisant une clause générale vague peut, dans cette mesure, être jugée abusive. Aux États-Unis, la constitutionnalité du Title III a été confirmée par les tribunaux inférieurs et, implicitement, par la Cour suprême dans l'affaire *Donovan*. Il s'agissait surtout de décider si la législation satisfaisait aux exigences relatives à l'obtention d'un mandat formulées dans le quatrième amendement.

Nous estimons que l'on ne saurait adopter une telle approche dans le contexte canadien. Comme le souligne Carr dans l'ouvrage intitulé *The Law of Electronic Surveillance*[119], l'établissement d'un rapport d'analogie avec le mandat de perquisition n'est pas très judicieux.

Il convient davantage dans le contexte canadien de souligner l'absence d'une disposition relative à l'obtention d'un mandat à l'article 8 de la *Charte canadienne des droits et libertés*. Bien que la Cour suprême du Canada ait néanmoins décidé qu'il y avait une présomption en faveur de l'obtention préalable d'un mandat avant qu'une fouille ou une perquisition raisonnable puisse être effectuée[120], il n'est pas clair que cette présomption vise une forme particulière de mandat.

Quoi qu'il en soit, il faut prévoir l'interception des appels des personnes inconnues. Celles-ci sont rangées dans deux catégories : (1) les personnes que l'on croit impliquées dans la commission de l'infraction mais qui ne sont pas identifiables; (2) les personnes qui, non seulement ne sont pas identifiables, mais dont l'existence peut être entièrement spéculative au moment de la demande d'autorisation. L'on pourrait fournir un exemple pour illustrer ces deux catégories. Pensons à une enquête en matière de stupéfiants.

Bien qu'il puisse être légitime de permettre l'interception des conversations tenues par ces personnes, la rédaction des dispositions législatives autorisant de telles interceptions soulève d'importants problèmes. Une clause générale trop vague est une invitation à l'interception inconsidérée des communications et à l'ingérence dans la vie privée. Alors que certaines dispositions sont rédigées de manière à exiger qu'un lien soit établi entre les infractions visées, par exemple «toutes personnes, dont l'identité est actuellement inconnue, fréquentant certains lieux aux fins de la commission de l'une des infractions désignées», de nombreuses dispositions ne sont pas ainsi formulées, par exemple «toutes personnes entrées en communication avec les personnes désignées aux lieux spécifiés»

118. *Code criminel*, alinéa 178.12(1)*e*).

119. J.G. Carr, *op. cit. supra*, note 67 (Suppl., 1983), p. 3-4.

120. *Supra*, note 37.

Si, selon nous, le droit à l'intimité de la vie privée ne peut être protégé que par une clause générale limitant l'interception aux conversations des personnes dont on croit qu'elles sont impliquées dans la commission de l'infraction, cette façon de procéder peut néanmoins créer de graves difficultés non seulement en ce qui concerne la rédaction de la clause mais également en ce qui concerne sa mise en œuvre. À titre d'illustration, nous reproduisons ci-dessous une clause générale employée couramment en Ontario :

> [TRADUCTION]
> 3b) Autorisation d'intercepter les communications privées de personnes dont l'identité est actuellement inconnue est, par les présentes, donnée, conformément aux modalités de la présente autorisation, pourvu qu'il y ait des motifs raisonnables et probables de croire que l'interception de telles communications privées pourra faire avancer l'enquête relative à l'une ou l'autre des infractions précisées au paragraphe 1 ci-dessus, peu importe que ces personnes décrites à l'alinéa 3a) participent ou non à ces communications privées[121].

En d'autres termes, la clause reprend le critère énoncé à l'alinéa 178.12(1)*e*) du *Code criminel*. Elle constitue une délégation illégale des fonctions du juge à la police comme l'a conclu la Cour d'appel de l'Ontario dans l'arrêt *R.* v. *Paterson, Ackworth and Kovach*[122]. On a souligné qu'il appartenait au juge de déterminer la catégorie de personnes dont les communications privées pouvaient faire l'objet d'une interception en vertu d'une clause générale. À notre avis, cette approche est la bonne, et le juge doit s'assurer que la clause générale est rédigée de façon à identifier les groupes pertinents, tels : les résidents permanents des lieux, les visiteurs habituels que l'on croit impliqués dans la commission de l'infraction, et ainsi de suite. Nous estimons que nos recommandations sont compatibles avec la décision rendue dans l'affaire *Paterson*.

Selon nous, l'emploi d'une clause générale n'est justifié que s'il permet l'interception des conversations des personnes faisant partie d'une catégorie dont on sait qu'elle est impliquée dans la commission de l'infraction. Par conséquent, la clause générale ne doit autoriser que l'interception des communications privées des personnes que l'on croit impliquées dans la commission de l'infraction mais qui ne sont pas identifiées au moment de la présentation de la demande d'autorisation.

Conformément à l'opinion que nous avons exprimée en ce qui concerne la portée de l'interception, nous sommes d'avis qu'il faudrait modifier la condition préliminaire de l'interception des communications privées des personnes (connues et identifiées) actuellement énoncée à l'alinéa 178.12(1)*e*) et remplacer l'expression «utile à l'enquête» par une disposition prévoyant la participation à l'infraction.

L'emploi d'une clause permettant l'installation d'un dispositif ailleurs qu'aux lieux désignés est un autre sujet de préoccupation lié aux clauses générales. Lorsque ce genre de disposition accompagne une clause générale très vague visant des personnes, le domaine d'application de l'autorisation devient considérable. Certes, les autorités doivent

---

121. Extrait d'une autorisation accordée par le juge McCart le 10 juin 1982 et citée dans l'affaire *Paterson*, *infra*, note 122, p. 147.

122. *R.* v. *Paterson, Ackworth and Kovach*, (1985) 18 C.C.C. (3d) 137.

pouvoir réagir rapidement au déplacement des personnes visées par l'autorisation, mais cette méthode devrait être limitée aux personnes désignées par l'autorisation afin de restreindre la portée de cette dernière à des limites raisonnables.

Cependant, afin de ne pas gêner inutilement la réalisation des objectifs légitimes de mise en application de la loi, tout en augmentant le pouvoir de surveillance des juges, nous estimons que l'agent de police devrait être tenu de se présenter à nouveau devant le juge afin de faire autoriser une utilisation plus large de la clause générale. À ce sujet, nous recommandons que la loi souligne le droit du juge d'insérer une condition dans l'autorisation afin d'exiger que des rapports périodiques lui soient présentés sur le déroulement de l'enquête. Nous ne prévoyons pas en faire une condition normale mais une telle disposition pourrait fort bien être considérée utile dans certaines enquêtes délicates. Mis à part ces recommandations, nous estimons que les articles 178.12 et 178.13 devraient demeurer inchangés en ce qui a trait à la délivrance de l'autorisation initiale.

RECOMMANDATIONS

26. Sous réserve des dispositions de la recommandation 27, l'autorisation devrait comporter une clause désignant, par leur nom ou autrement, les personnes à l'égard desquelles il existe des motifs raisonnables de croire que l'interception de leurs communications privées pourrait faire avancer l'enquête sur l'infraction en cause, en raison de leur participation à cette infraction.

27. L'autorisation devrait en outre pouvoir comporter une clause permettant l'interception des communications privées d'une catégorie de personnes non désignées, s'il existe des motifs raisonnables de croire que cette interception pourrait faire avancer l'enquête sur l'infraction en cause, en raison de leur participation à cette infraction.

28. Sous réserve des dispositions de la recommandation 29, l'autorisation devrait restreindre les interceptions à des lieux désignés.

29. L'autorisation devrait pouvoir comporter une clause permettant l'interception de communications privées dans des lieux non désignés, mais fréquentés par des personnes connues et identifiées dans l'autorisation. Seules devraient toutefois pouvoir être interceptées dans ces lieux les communications privées auxquelles la personne connue et identifiée participe, à moins qu'un mandataire spécialement désigné à cette fin n'ait demandé par écrit au juge qui a autorisé initialement la demande de modifier celle-ci dans les plus brefs délais. La demande de modification doit être accompagnée de l'affidavit de l'agent de police énonçant les motifs de l'interception dans ces lieux, le nom des personnes dont les communications privées sont susceptibles d'être interceptées ainsi que les raisons pour lesquelles l'interception dans ces lieux est nécessaire. Le juge peut refuser de modifier l'ordonnance ou y apporter une modification dont l'entrée en vigueur est fixée à la date où la

première interception a eu lieu à la nouvelle adresse désignée, à moins qu'il ne soit pas convaincu que la demande a été présentée dans les plus brefs délais, auquel cas la modification pourra prendre effet à la date que le juge estimera opportune.

30. La loi devrait énumérer les conditions *pouvant* figurer dans l'autorisation, par exemple :

a) l'obligation d'informer périodiquement le juge ayant autorisé l'interception, au sujet de l'identité des personnes dont les communications sont interceptées en vertu d'une autorisation générale;

b) l'obligation d'informer périodiquement le juge ayant autorisé l'interception, au sujet des lieux, non désignés précisément dans l'autorisation, où l'on se livre à des interceptions.

F. L'entrée clandestine

Par entrée clandestine nous entendons l'introduction dans un lieu privé, par des agents chargés de l'application de la loi, sans le consentement de l'occupant ou à son insu afin d'installer un dispositif d'écoute. D'ordinaire, il s'agit d'un émetteur radio capable de retransmettre les communications orales à un poste situé à l'extérieur du lieu où l'enregistrement des conversations peut être effectué. Parfois, les agents s'introduisent clandestinement à la seule fin d'installer un dispositif auxiliaire pour permettre l'interception des communications téléphoniques. Mais comme cela n'est pas nécessaire d'habitude, on a rarement recours à l'entrée clandestine pour ce genre d'installation. Suite aux décisions rendues par la Cour suprême du Canada dans les arrêts *Lyons* c. *La Reine*[123] et *Le renvoi sur l'écoute électronique*[124], publiés le 20 décembre 1984, l'on peut résumer l'état actuel du droit sur cette question comme suit :

a) À moins que l'autorisation ne contienne des réserves au sujet de l'entrée clandestine ou ne l'interdise, l'autorisation permet, par voie d'interprétation nécessaire, à toute personne agissant aux termes de l'autorisation de s'introduire en tout lieu où des communications privées doivent être interceptées, afin d'y installer un dispositif d'écoute autorisé ou de le réparer, pourvu qu'une telle entrée soit nécessaire pour mettre en œuvre l'autorisation.

b) L'interception comprend l'installation du dispositif et, par conséquent, une interception n'est légalement effectuée, au sens de l'alinéa 178.16(1)*a*), que si l'installation du dispositif était légale.

c) Cependant, le mot «légal» signifie «conformément aux dispositions de la Partie IV.1» et, donc, une entrée clandestine en vue d'installer un dispositif d'écoute pour mettre en œuvre une autorisation étant légale, l'interception serait effectuée légalement.

123. *Lyons* c. *La Reine*, [1984] 2 R.C.S. 631.

124. *Le renvoi sur l'écoute électronique*, [1984] 2 R.C.S. 697.

La commission McDonald[125] s'est prononcée en faveur d'une loi prévoyant expressément l'autorisation de l'entrée clandestine en matière de sécurité nationale. Cette autorisation était assujettie à deux conditions. Premièrement, le droit d'introduction devait être explicite et assorti de certaines réserves et, deuxièmement, l'introduction ne pouvait être autorisée par un juge que dans certaines circonstances.

La commission McDonald, convaincue que l'entrée clandestine est légitime en matière de surveillance électronique, a également fait des recommandations concernant l'enquête criminelle[126]. Ces recommandations ne visent toutefois pas les fouilles, les perquisitions et les saisies en général[127]. Comme nous l'avons indiqué précédemment, la Commission était d'avis que l'entrée clandestine n'était pas légale pour l'instant. Voici ses recommandations à ce sujet :

> NOUS RECOMMANDONS QUE l'article 178.13 du Code criminel soit modifié de manière à permettre aux agents de la paix qui exécutent les autorisations accordées en vertu de cet article de prendre les mesures raisonnablement nécessaires pour pénétrer dans des locaux ou prendre des biens en vue d'examiner ces locaux ou ces biens avant d'installer un dispositif ou afin d'installer, d'entretenir ou de retirer un dispositif d'interception, à condition que le juge qui accorde l'autorisation y indique
>
> *a*) les méthodes à employer pour exécuter l'autorisation;
>
> *b*) que rien ne doit être fait qui puisse causer aux locaux des dommages graves qui ne seraient pas réparés;
>
> *c*) qu'on ne doit pas employer la force physique, ni menacer d'y recourir, contre qui que ce soit[128].

La Commission a également souligné qu'aux États-Unis, en dépit d'une décision rendue par la Cour suprême des États-Unis, laquelle avait décidé que l'entrée clandestine était légale, l'on envisageait d'adopter un texte constitutionnel pour régir l'entrée clandestine. La commission McDonald cite la déclaration faite par le procureur général adjoint, division criminelle, devant le comité judiciaire du Sénat, selon laquelle,

> aux États-Unis, malgré l'affirmation, par la Cour suprême, du pouvoir implicite d'entrer, le gouvernement a présenté au Congrès un projet de loi qui prévoit *expressément* le pouvoir d'entrer et des sauvegardes propres à assurer qu'il ne sera recouru à ces méthodes que lorsque, comme le déclarait le procureur général adjoint, division criminelle, «elles auront été jugées raisonnables et nécessaires par un magistrat informé et impartial»[129].

De plus, en dépit de la décision rendue par la Cour suprême des États-Unis, le ministère de la Justice des États-Unis a décidé de demander une autorisation judiciaire pour les entrées clandestines.

---

125. Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada, *Deuxième rapport : la liberté et la sécurité devant la loi*, 2 vol., Ottawa, Ministère des Approvisionnements et Services, 1981, président : le juge D.C. McDonald (ci-après appelé le rapport McDonald).

126. *Id.*, vol. 2, p. 1081-1082.

127. *Id.*, vol. 1, p. 148-149; vol. 2, p. 1078.

128. *Id.*, vol. 2, p. 1081-1082, recommandation 265.

129. *Id.*, vol. 1, p. 182.

La seule opinion dissidente exprimée au sujet de la nécessité d'adopter une législation prévoyant l'autorisation de l'entrée clandestine, est le rapport préparé par le comité McLeod[130] en réponse au rapport McDonald. Le comité McLeod estimait que l'entrée clandestine était légale et qu'il n'était pas nécessaire d'adopter des dispositions pour régir cette question. Bien qu'en définitive, le comité McLeod ait eu raison de conclure que l'entrée clandestine n'était pas illégale, pour les raisons exposées ci-dessous, nous estimons que si l'entrée clandestine doit être autorisée, elle doit faire l'objet d'une loi précise.

Comme nous l'avons indiqué antérieurement, l'une des questions dont la Cour suprême a été saisie avait initialement été soumise à la Cour d'appel de l'Alberta[131]. Le juge en chef McGillivray et le juge Harrandence de la Cour d'appel étaient d'avis que l'entrée clandestine n'était légale que si elle était expressément permise par le juge dans l'autorisation. Les deux juges sentaient la nécessité d'un contrôle judiciaire exercé grâce à l'adjonction des conditions appropriées[132].

Le juge Harrandence avait précisé dans quelle circonstance l'entrée clandestine devait être autorisée :

> [TRADUCTION]
> Selon moi, si un juge d'une cour supérieure saisi d'une demande d'autorisation présentée en vertu de la Partie IV.1 du *Code criminel*, décide que les intérêts de la société ne peuvent être servis *que* par l'interception des communications privées qui, à son tour, ne peut être effectuée efficacement *que* par l'installation d'un dispositif d'écoute sur une propriété privée, il lui faut adapter le common law afin de tenir compte des circonstances de la vie moderne en autorisant l'entrée clandestine ou un stratagème susceptible de permettre l'installation d'un dispositif d'écoute sur cette propriété[133]. [Mots soulignés dans le jugement original]

Les mêmes préoccupations ont été exprimées par la majorité des juges dans l'arrêt *Lyons* c. *La Reine*. Le juge Estey, tout en décidant que le droit d'entrée ne devait pas être nécessairement explicite dans l'autorisation, a estimé qu'il s'agissait d'une question devant être tranchée par le juge accordant l'autorisation.

> Compte tenu de l'économie de la Partie IV.1, de la portée du pouvoir accordé au tribunal, de l'importance du sujet et du caractère vital du rôle de gardien de l'intérêt public attribué par le législateur au tribunal, celui-ci devra souvent insérer dans sa réponse à la demande d'autorisation les «modalités que le juge estime opportunes dans l'intérêt du public» conformément à l'alinéa 178.13(2)*d*)[134].

---

130. *Rapport du comité fédéral-provincial des fonctionnaires chargés de la justice pénale au sujet du Rapport de la Commission McDonald*, Ottawa, Division des communications, Solliciteur général du Canada, 1983, président : R.M. McLeod, c.r. (ci-appelé le rapport du comité McLeod).

131. *Reference re an Application for an Authorization*, (1983) 10 C.C.C. (3d) 1 (C.A. Alb.).

132. *Id.*, p. 14-15, commentaires du juge en chef McGillivray.

133. *Id.*, p. 28.

134. *Supra*, note 123, p. 671.

Ajoutons que dans l'énoncé de politique intitulé *Le Droit pénal dans la société canadienne*[135], le principe suivant a été adopté : «Le droit pénal doit prévoir et définir clairement les pouvoirs nécessaires à la conduite des enquêtes criminelles ...».

La Commission de réforme du droit s'est déjà penchée sur le problème de l'entrée clandestine. D'après l'une des recommandations du document de travail 30,

> [l]a modification des règles relatives aux fouilles, aux perquisitions et aux saisies, afin de permettre les activités clandestines de la police constituerait une atteinte grave aux mécanismes de protection que ces règles comportent. En l'absence de preuve établissant de façon convaincante la nécessité de tels sacrifices, les règles de procédure relatives aux enquêtes en matière criminelle ou en matière connexe ne devraient pas être modifiées[136].

L'auteur a fait remarquer que ni le common law ni la loi n'autorisaient l'entrée clandestine aux fins d'effectuer une fouille, une perquisition ou une saisie. Le document de travail traite, pour l'essentiel, du problème des investigations exploratoires menées par la police en vue de recueillir des renseignements. Il n'aborde pas la question de la surveillance électronique. Quoi qu'il en soit, le critère suggéré pour l'exception pourrait s'appliquer, à savoir : Y a-t-il une preuve établissant de façon convaincante la nécessité des entrées clandestines en matière de surveillance électronique?

Les chiffres que nous avons en main sont ambigus et manquent d'exactitude. Nous aurions donc tort de nous y fier pour décider si l'entrée clandestine est nécessaire. Nous ne croyons pas nous tromper en disant que l'entrée clandestine se produit relativement rarement. Cela n'est pas étonnant. L'entrée clandestine représente certains dangers pour l'enquête. Les agents peuvent être pris pendant l'installation des dispositifs d'écoute ou ceux-ci peuvent être découverts. L'entrée clandestine peut également présenter des difficultés et comporter une dépense de temps et d'énergie que seule peut justifier une probabilité élevée que des preuves que l'on n'aurait pu obtenir par l'écoute téléphonique, plus facile à effectuer, seront recueillies. Néanmoins, l'entrée clandestine a été employée en matière de surveillance électronique, et elle a donné de bons résultats. D'autres dispositifs, tels les microphones paraboliques, sont non seulement moins efficaces, mais représentent un risque plus élevé d'immixtion dans les communications des tiers innocents.

Dans le document de travail 30, deux importants problèmes ont été associés à l'entrée clandestine en matière de fouille, de perquisition et de saisie. Premièrement, le recours à l'entrée clandestine était souvent bien fondé dans des cas où il n'existait pas encore de motifs permettant la délivrance d'un mandat de perquisition. Mais cela ne susciterait aucune difficulté en matière de surveillance électronique puisque l'entrée

---

135. *Op. cit. supra*, note 35, p. 69.

136. Document de travail sur les fouilles, les perquisitions et les saisies, *op. cit. supra*, note 47, p. 296, recommandation 42.

clandestine ne serait permise qu'aux fins de la mise en œuvre de l'autorisation. Bien qu'il soit arrivé à la police de s'introduire subrepticement dans un lieu afin d'examiner s'il était possible d'y installer des microphones, cette façon de recueillir des renseignements ne peut être dissociée d'une décision judiciaire portant qu'il y a des motifs justifiant l'autorisation d'intercepter des communications privées. Comme il a été souligné dans le document de travail 30 «le fait de permettre à la police de s'introduire afin de vérifier l'existence même des motifs raisonnables rendrait illusoires les mécanismes de protection contre les atteintes injustifiées[137]».

Le document de travail 30 traite d'un second problème, à savoir celui de la responsabilité et de la vérification des autorisations. Il s'agit d'un grave problème dans un régime où les fouilles, les perquisitions et les saisies sont assujetties à des exigences relatives à l'avis préalable à l'entrée, à l'obligation de fournir certains documents à l'occupant des lieux visés et à celle de lui permettre d'assister à la perquisition. La modification de ces règles «entraverai[t] grandement les mécanismes de protection que comportent les règles relatives au mandat[138]». Il convient cependant de rappeler que ces problèmes ne se posent pas en matière de surveillance électronique. Même l'écoute téléphonique, telle qu'elle est autorisée actuellement, est effectuée secrètement et est très différente de la fouille, de la perquisition ou de la saisie ordinaire. La décision de principe autorisant la surveillance électronique est en réalité la permission de procéder à une enquête secrète. En matière de surveillance électronique, la véritable question est la suivante : quelle forme d'immixtion secrète devrions-nous permettre et quelle garantie devrions-nous prévoir? Il ne s'agit pas de mettre en veilleuse le problème de la responsabilité mais, comme l'a souligné le document de travail 30, c'est un problème de plus en plus aigu en matière de surveillance électronique[139].

Comme nous sommes en faveur d'un régime un peu plus ouvert de manière générale, nous aborderons certaines de ces préoccupations. D'abord, en ce qui concerne l'entrée clandestine, il serait tout à fait indiqué de prévoir une forme spéciale d'avis lorsque aucune accusation n'est portée, et que de ce fait, l'on ne peut pas respecter le principe de la responsabilité ni vérifier le bien-fondé de l'autorisation au procès. Après avoir examiné ce problème, dans son ouvrage intitulé *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance*, l'American Bar Association a tiré la conclusion suivante :

> [TRADUCTION]
> On pourrait faire élaborer des règles concernant l'état à dresser de manière à réfuter les aspects les plus convaincants de l'objection formulée à l'encontre du caractère clandestin de la surveillance électronique. Autrement dit, l'entrée clandestine ne serait clandestine qu'au début. Cette objection n'a pas non plus à être déterminante[140].

137. *Id.*, p. 303.

138. *Ibid.*

139. *Id.*, p. 305.

140. *Op. cit. supra*, note 50, p. 92.

Mais qu'en est-il du droit à la vie privée? Quelle est la gravité de l'atteinte portée par l'entrée clandestine? L'entrée elle-même n'est pas censée être décelée, et d'ordinaire, elle est effectuée aussi discrètement que possible, bien que tel ne soit pas toujours le cas[141]. La véritable immixtion dans la vie privée de l'occupant a lieu plus tard, après l'interception des communications faites dans l'intimité, soit à la maison, soit au bureau, grâce aux dispositifs d'écoute, comme l'ont souligné le juge en chef McGillivray[142] dans l'arrêt *Reference re an Application for an Authorization* et le juge Estey dans l'affaire *Lyons*[143].

À la maison ou au bureau, les gens s'expriment librement sans penser que leurs paroles pourraient être rapportées même au téléphone. L'atteinte portée à l'intimité de la vie privée par l'entrée clandestine en vue d'installer un dispositif d'écoute est si grave qu'elle ne devrait être autorisée que dans des cas très précis.

Il faudrait, au moins, que le droit de s'introduire clandestinement ne soit pas prévu implicitement dans chaque autorisation mais qu'il dépende du juge qui décidera si, eu égard à la gravité de l'infraction visée et à la probabilité d'obtenir ainsi des preuves, l'immixtion projetée est justifiée. En plus, il faudrait poser des conditions comme celles que proposait la commission McDonald dans son projet de loi sur la sécurité nationale.

Dans de récents jugements, la Cour suprême du Canada ne s'est pas prononcée sur les répercussions que pourrait avoir sur l'entrée clandestine l'article 8 de la *Charte canadienne des droits et libertés*.

À ce propos, il convient de souligner que dans l'arrêt *Dalia* v. *United States*[144], la Cour a statué qu'il n'y avait pas dérogation aux dispositions du quatrième amendement. Dans cette affaire, le mandat portait que l'interception de toutes les communications orales de Dalia [TRADUCTION] «faites à son bureau» était autorisée. La Cour a conclu que l'autorisation comportait implicitement la permission d'entrer clandestinement chez Dalia, et qu'il n'y avait pas là atteinte au quatrième amendement. La Cour était convaincue que le Congrès savait très bien qu'il confiait au juge le pouvoir connexe d'autoriser les entrées clandestines en lui confiant la tâche de vérifier et d'approuver les demandes d'écoute clandestine. Comme dans le cas des mandats de perquisition, les textes constitutionnels n'exigent pas que le mandat autorisant la surveillance électronique en précise les moyens d'exécution.

Nous estimons que l'arrêt *Hunter* c. *Southam Inc.*[145], dans lequel la Cour suprême du Canada a exprimé sa préférence pour l'autorisation judiciaire préalable afin de se

141. Il semble y avoir des cas où un avertisseur d'incendie ait été déclenché afin de faire évacuer les lieux et de permettre aux autorités d'installer le dispositif.

142. *Supra*, note 131, p. 12.

143. *Supra*, note 123.

144. *Dalia* v. *United States*, 441 U.S. 238 (1979).

145. *Supra*, note 37.

conformer aux exigences de l'article 8 de la *Charte canadienne des droits et libertés*, milite fortement en faveur d'un régime législatif dans lequel le droit de s'introduire subrepticement serait implicite tant dans la loi que dans l'autorisation[146].

Selon la majorité des avis exprimés au cours des consultations, il n'y a pas de raison pour limiter l'entrée clandestine à certaines infractions graves. Il appartiendra au juge de trancher la question à l'aide de certaines lignes directrices. Néanmoins, à notre avis, l'entrée clandestine devrait être réservée pour les cas graves dans lesquels il y a une forte probabilité d'obtenir des preuves pertinentes.

Nous croyons fermement que l'entrée clandestine ne devrait être effectuée qu'en vertu d'une autorisation accordée aux termes des dispositions de la Partie IV.1 et non en vertu d'un autre acte judiciaire comme le mandat de perquisition. Comme l'a fait remarquer la Cour d'appel de l'Ontario dans l'arrêt *R.* v. *McCafferty*[147], le mandat de perquisition doit être interprété de façon stricte et ne peut autoriser une fouille ou une perquisition générales, ni l'installation d'un dispositif d'écoute.

De même, l'entrée clandestine effectuée en vertu d'une autorisation ne permet pas qu'une perquisition dans les lieux soit effectuée, bien que des renseignements obtenus de façon tout à fait fortuite à l'occasion de l'entrée clandestine puissent justifier la présentation d'une demande de mandat de perquisition dont l'exécution sera effectuée de la manière habituelle.

Un régime d'autorisation préalable suppose évidemment que la police révélera au juge qui délivre l'autorisation qu'elle entend faire une entrée clandestine. Nous nous sommes demandés quels renseignements il fallait fournir au juge et plus particulièrement s'il fallait lui dévoiler les moyens que la police prévoyait utiliser pour effectuer cette entrée. On nous a fait valoir avec insistance que d'une part, une certaine souplesse était nécessaire car la police doit pouvoir adapter ses méthodes à des conditions changeantes et que, d'autre part, le juge, ne disposant pas des connaissances techniques nécessaires, ne serait pas en mesure de statuer sur la pertinence d'une méthode ni même de se prononcer sur l'opportunité d'utiliser cette méthode plutôt qu'une autre. Cependant, l'usage de moyens impropres à cette fin, tel que le déclenchement d'un avertisseur d'incendie en vue de faire évacuer un édifice, demeure au premier plan des préoccupations. Après en avoir discuté longuement, nous avons décidé d'opter pour la souplesse et de ne pas exiger que les méthodes envisagées soient précisées dans la demande. Si des abus étaient constatés au cours des années qui viennent, cette prise de position devrait bien sûr être reconsidérée. Il n'y a cependant pas de raison de s'alarmer à l'heure actuelle. Néanmoins, il conviendrait d'investir le juge qui délivre l'autorisation du pouvoir de statuer sur certaines méthodes s'il le juge opportun.

---

146. Il convient peut-être de souligner que le juge en chef Dickson, qui a rendu le jugement pour la Cour dans l'arrêt *Southam*, *supra*, note 37, était dissident tant dans l'affaire *Lyons*, *supra*, note 123, que dans l'affaire *Le renvoi sur l'écoute électronique*, *supra*, note 124, parce qu'il était d'avis que la Partie IV.1 du *Code criminel* n'autorisait pas l'entrée clandestine. Même dans son rapport, le comité McLeod a admis que la Charte pouvait soulever des problèmes en ce qui concerne l'entrée subreptice.

147. *R.* v. *McCafferty*, (1984) 13 W.C.B. 143 (C.A. Ont.).

RECOMMANDATIONS

31. Le juge qui délivre l'autorisation devrait être investi du pouvoir d'autoriser l'introduction dans un lieu privé sans le consentement de l'occupant en vue de l'installation, de l'enlèvement ou de la réparation d'un dispositif électromagnétique, acoustique, mécanique ou autre.

32. Le juge qui délivre l'autorisation ne devrait pouvoir donner cette autorisation que lorsque les circonstances entourant l'infraction sont graves et que l'obtention d'éléments de preuve pertinents est très probable.

33. La demande d'autorisation qui comprend l'autorisation de faire une entrée clandestine devrait énoncer les motifs pour lesquels cette entrée est nécessaire et préciser pourquoi les autres moyens moins attentatoires à la vie privée ne seraient pas suffisants dans ce cas.

34. Devrait constituer une infraction le fait d'entrer dans des lieux privés sans le consentement de l'occupant en vue d'installer, de réparer ou d'enlever un dispositif électromagnétique, acoustique, mécanique ou autre et sans l'autorisation accordée en vertu de la Partie IV.1 du *Code criminel*. Devrait également constituer une infraction, le fait de retirer des lieux quelque chose que ce soit au moment de l'entrée.

35. Le policier qui effectue l'entrée clandestine ne devrait pas être autorisé à recourir à la force contre quiconque pour entrer dans les lieux ou en sortir, sauf dans la mesure nécessaire pour assurer sa propre protection ou celle des autres.

36. Le juge qui délivre l'autorisation peut ordonner ou interdire l'utilisation de certains moyens pour l'entrée clandestine.

37. Après l'enquête, le propriétaire et l'occupant des lieux devraient être avisés de l'entrée clandestine, et copie de l'ordonnance autorisant l'entrée devrait leur être donnée.

38. Des mesures raisonnables devraient être prises en vue de la réparation de tout dommage causé aux lieux ou de l'indemnisation du propriétaire pour tout dommage important non réparé.

39. La consommation d'une faible quantité d'électricité pour assurer le fonctionnement du dispositif ne devrait pas constituer une infraction criminelle.

G. Les renouvellements

Le caractère attentatoire de la surveillance électronique est également fonction de la durée de l'immixtion. Pendant certaines enquêtes, l'interception peut se prolonger durant des mois. La *Loi de 1977 modifiant le droit pénal* a porté la durée de l'autorisation de trente à soixante jours[148]. Bien que l'alinéa 178.13(2)*e*) du *Code criminel* prévoie que l'ordonnance est valide «pour la période de soixante jours au plus qui y est indiquée», dans les faits, il est très rare qu'une autorisation soit accordée pour une période de moins de soixante jours. La situation aux États-Unis est différente. La loi[149] prévoit une durée maximale de trente jours et exige que l'ordonnance contienne une clause portant que l'interception ne doit pas se poursuivre au-delà de la période nécessaire pour atteindre les objectifs de l'autorisation. La durée moyenne des autorisations accordées aux États-Unis semble varier d'État en État, et même, de comté en comté. Toutefois, dans la plupart des cas, la durée réelle se situe très près de la durée maximale permise par la loi. L'efficacité de cette clause n'est pas prouvée puisqu'en général le dispositif fonctionne pendant toute la durée autorisée[150]. (Aucune donnée statistique n'est recueillie aux termes de l'article 178.22 du *Code criminel* en ce qui concerne la durée de l'interception).

La loi canadienne permet le renouvellement de l'autorisation pour une période de soixante jours[151]. L'objet évident de la fixation d'un délai est de prévoir une limite temporelle à l'interception des communications privées afin que l'autorisation ne devienne pas une sorte de mandat général à durée illimitée. Par ces dispositions, le législateur reconnaît que certaines enquêtes peuvent, à bon droit, demander plus de soixante jours. Toutefois, conformément au principe de la modération, la nécessité de prolonger cette immixtion dans la vie privée doit être prouvée.

Quoi qu'il en soit, en raison d'une jurisprudence récente, la police demandera rarement le renouvellement d'une autorisation. Elle cherchera plutôt à obtenir une nouvelle autorisation même si des modifications très mineures seulement sont envisagées. Dans l'arrêt *R.* v. *Badovinac*[152], la Cour a décidé qu'un renouvellement ne pouvait que prolonger le délai accordé initialement et n'autorisait pas [TRADUCTION] «l'extension ni la modification d'aucune façon des modalités de l'autorisation[153]». Comme l'a fait remarquer le juge dans le jugement *R.* v. *Pleich*[154], la législation qui favorise l'obtention d'une nouvelle autorisation plutôt que celle d'un renouvellement n'est pas sans avoir

148. *Loi de 1977 modifiant le droit pinal*, S.C. 1976-1977, chap. 53, par. 9(3).

149. Title III, *supra*, note 67, par. 2518(4) et (5).

150. *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications, 1983*, Washington, D.C., Administrative Office of the United States Courts, 1983 (ci-après appelé le rapport Wiretap).

151. *Code criminel*, par. 178.13(4).

152. *R.* v. *Badovinac*, (1977) 34 C.C.C. (2d) 65 (C.A. Ont.).

153. *Id.*, p. 70.

154. *R.* v. *Pleich*, (1980) 55 C.C.C. (2d) 13 (C.A. Ont.).

certaines conséquences. Même si, tout compte fait, les conditions d'obtention d'une autorisation, énoncées à l'article 178.12, peuvent être plus exigeantes que celles d'un renouvellement, ces dernières sont axées véritablement sur l'opportunité de poursuivre l'enquête par écoute électronique au-delà de la limite prévue par la loi. Le paragraphe 178.13(3) dispose qu'une autorisation peut être renouvelée (1) sur présentation d'une demande *ex parte* (2) à laquelle est joint un affidavit d'un agent de la paix ou d'un fonctionnaire public énonçant les raisons et la période pour laquelle le renouvellement est demandé, tous les détails relatifs aux interceptions qui ont été faites et tous les renseignements obtenus au cours de ces interceptions, le nombre de cas où une demande de renouvellement a été faite et où elle a été retirée ou refusée ainsi que (3) tous les renseignements que le juge peut exiger[155].

Comme il a été souligné dans l'arrêt *R.* v. *Pleich*[156], bien que la divulgation complète à laquelle on s'attend au moment de la présentation d'une demande d'autorisation subséquente en vertu de l'article 178.12 exigerait probablement que l'on fournisse le genre de renseignements mentionnés au paragraphe 178.13(3), la loi reste muette sur ce point.

À notre avis, la loi doit être modifiée de façon que le renouvellement puisse être obtenu dans les cas où l'on ne prévoit apporter que des modifications mineures à l'autorisation initiale et où la même enquête se poursuit. En revanche, si l'enquête est si avancée que des modifications importantes sont nécessaires, une nouvelle autorisation devrait être demandée. Cependant, dans ce dernier cas, la portée de la première enquête doit être révélée pour que le juge soit en mesure d'apprécier correctement le bien-fondé de la demande.

Nous estimons également que plus l'enquête dure longtemps, plus l'immixtion dans la vie privée est importante et donc plus il est nécessaire d'assurer un examen judiciaire et de veiller à ce que les fonctionnaires chargés de l'application de la loi s'acquittent de leurs obligations en vertu du principe de la responsabilité. Par conséquent, nous proposons que la durée normale du renouvellement soit fixée à trente jours, à moins qu'il ne soit établi qu'une période plus longue, dont la durée maximale serait soixante jours, est nécessaire. Nous estimons qu'une telle approche est davantage compatible avec le principe de la modération. Bien sûr, des mesures doivent être prises pour veiller à ce que la police ne présente pas une demande d'autorisation à la seule fin d'obtenir une durée plus longue.

RECOMMANDATIONS

40. Lorsque, à la connaissance du mandataire désigné ou du souscripteur de l'affidavit présenté à l'appui de la demande d'autorisation, une autorisation a déjà été donnée au sujet de la même enquête ou d'une enquête connexe, la demande devrait comporter les renseignements mentionnés à l'alinéa 178.13(3)*b*) du *Code*.

155. *Code criminel*, par. 178.13(3).

156. *Supra*, note 154.

41. Toute autorisation renouvelée devrait pouvoir comporter le nom des personnes antérieurement visées par l'autorisation mais qui n'y était pas nommées.

42. Toute autorisation renouvelée peut permettre l'interception, dans de nouveaux lieux, de communications auxquelles participent des personnes visées par l'autorisation initiale.

43. Des modifications mineures peuvent être apportées aux conditions de l'autorisation à l'occasion d'un renouvellement, notamment les suivantes :

a) la désignation différente ou plus précise de personnes ou de lieux;

b) la modification des moyens d'interception ou la désignation de nouveaux moyens;

c) la modification des infractions visées par l'autorisation initiale ou l'adjonction d'infractions ayant un rapport manifeste avec celles-ci et entrant dans le cadre de la même enquête.

44. Toute autorisation renouvelée devrait pouvoir comporter des conditions qui ne faisaient pas partie de l'autorisation initiale et qui sont destinées à restreindre l'interception de communications n'ayant aucun rapport avec l'infraction.

45. Aucune autorisation ne devrait pouvoir être renouvelée pour une période de plus de trente jours ou, si l'on établit l'existence de circonstances particulières, de plus de soixante jours. L'expression «circonstances particulières» désigne ici des circonstances telles que vraisemblablement l'enquête ne sera pas terminée au bout de trente jours *et* qu'il serait impossible en pratique d'obtenir un autre renouvellement dans les trente jours. Lorsqu'un juge délivre un renouvellement d'une durée supérieure à trente jours, il devrait être tenu de préciser, au recto de l'autorisation, les raisons qui motivent sa décision, ainsi que les circonstances particulières de l'enquête.

46. Dans tous les cas visés à la recommandation 45, le juge devrait être tenu de s'assurer que l'obtention d'un renouvellement de l'autorisation serait impossible dans les circonstances. Le juge ne devrait en aucun cas accorder l'autorisation s'il a des motifs de croire que l'on cherche à échapper aux exigences de la recommandation 45. Si le renouvellement ne peut être obtenu pour la seule raison que le précédent renouvellement ou l'autorisation n'est plus en vigueur, la nouvelle autorisation devrait avoir une durée de trente jours à moins que l'on démontre l'existence de circonstances particulières.

47. La loi devrait énoncer une liste des conditions susceptibles d'être incluses dans l'autorisation renouvelée, par exemple les suivantes :

a) la fin obligatoire de l'interception lorsque le but de l'autorisation initiale est atteint;

b) l'obligation de présenter toute demande ultérieure de renouvellement ou d'autorisation au juge qui a accordé l'autorisation ou le renouvellement initiaux.

III. La vérification de l'autorisation et le secret

A. Introduction

Il est essentiel dans le système anglo-canadien que les actes judiciaires soient publics afin qu'ils soient soumis à l'examen du public et à celui des tribunaux supérieurs. L'on ne s'étonnera donc pas que l'une des caractéristiques importantes de la Partie IV.1 du *Code criminel*, à savoir le secret entourant la demande d'autorisation et la réticence des juges à statuer sur l'à-propos de la demande, fasse aujourd'hui l'objet de discussion sur la scène constitutionnelle[157]. Les experts-conseils du ministère public et de la police nous ont expliqué à maintes reprises que les contrôles internes prévus au moment de la présentation de la demande, l'obligation de faire examiner la demande d'autorisation par les fonctionnaires supérieurs chargés de l'application de la loi et, par la suite, par le procureur de la Couronne, font que seules les demandes bien fondées sont présentées. Mais, selon nous, là n'est pas la question, en particulier lorsqu'il s'agit d'une méthode d'enquête aussi attentatoire à la vie privée, comme l'a dit le juge Jackson dans l'arrêt *Johnson* v. *United States*[158], lequel portait sur les garanties contre les fouilles, les perquisitions et les saisies abusives du quatrième amendement. Un magistrat neutre et indépendant, plutôt qu'un fonctionnaire ayant un rôle à jouer dans l'enquête[159], devrait statuer sur ces demandes.

Si donc l'importance de la participation d'un fonctionnaire judiciaire impartial au moment de la présentation de la demande est admise, à titre de garantie contre les immixtions abusives dans la vie privée, on peut se demander, à juste titre, pourquoi il y aurait un autre examen judiciaire au moment de la production de la preuve. Le juge Dickson dans l'arrêt *Le procureur général de la Nouvelle-Écosse* c. *MacIntyre*[160] a exposé les raisons motivant l'application du principe de la transparence après l'exécution d'un mandat de perquisition. Il s'agit, semble-t-il, d'appliquer la règle de la responsabilité judiciaire afin de protéger le public contre tout abus dans l'exercice des pouvoirs très larges et très attentatoires à la vie privée dont est investie la police en matière de fouille ou de perquisition et d'écoute clandestine. L'idéal serait peut-être que chaque ordonnance autorisant l'écoute clandestine soit soumise à un examen judiciaire subséquent afin de décider s'il y a eu un abus. Cependant, cette solution n'est pas réalisable et présente, sans doute, peu d'intérêt lorsqu'il s'agit d'apprécier la probabilité d'un abus. Du reste, les ressources nécessaires pour effectuer un examen minutieux de ces procédures ne sont prévues, pour l'essentiel, que dans le cadre des procès criminels, lorsque la liberté individuelle est en jeu. C'est à ce stade seulement que la victime de

157. Selon l'interprétation donnée à l'alinéa 2*b*) de la *Charte canadienne des droits et libertés*, dans l'arrêt *Re Southam Inc. and The Queen (No. 1)*, (1983) 3 C.C.C. (3d) 515 (C.A. Ont.).

158. *Johnson* v. *United States*, 333 U.S. 10 (1948), cité dans *R.* v. *Rao*, *supra*, note 46.

159. *Id.*, p. 13-14.

160. *Supra*, note 96, p. 183-187 (R.C.S.), p. 144-147 (C.C.C.).

l'immixtion a l'intérêt et les renseignements lui permettant de contester la procédure suivie et que l'État a l'intérêt suffisant pour défendre correctement l'action prise par les autorités. En définitive, le procès criminel fait office de bouclier contre les atteintes à l'intimité personnelle. L'idée que les actes des autorités seront soumis à un examen minutieux pendant le procès préserve l'intégrité de tout le système et protège le public en général contre les immixtions abusives. Bien sûr, un examen plus minutieux entraîne des coûts. Les procès peuvent être prolongés, les techniques d'investigation de la police peuvent être révélées, certains coupables peuvent être mis en liberté. Il s'agira donc d'apprécier la nécessité de protéger le droit à la vie privée par rapport aux coûts qu'elle entraîne, compte tenu du fait qu'en raison de ces coûts, le procès criminel n'est pas un moyen efficace de contrôler le déroulement de l'enquête en général et, en particulier, en matière de surveillance électronique.

B. La vérification de l'autorisation

Les dispositions actuelles du *Code criminel* n'énoncent pas expressément les motifs justifiant la vérification de l'autorisation. Celle-ci est bien évidemment liée à l'admissibilité de la preuve. Même si certaines voies de recours civiles pourraient être invoquées, les questions importantes sont soulevées dans le cadre du procès criminel.

À l'alinéa 178.16(1)*a*), la condition de base de l'admissibilité de la preuve est que l'interception soit effectuée légalement. (L'admission de la preuve par consentement de l'une des parties est également prévue à l'alinéa 178.16(1)*b*) mais cette disposition soulève d'autres questions.) L'alinéa 178.16(1)*a*) correspond à peu près à l'article 2515 du Title III. Selon l'interprétation que lui ont donnée les tribunaux, les éléments de preuve sont recevables lorsque l'une des parties à la communication consent à ce qu'elle soit interceptée. L'interception n'est donc pas dans ce cas illégale en vertu de l'alinéa 178.11(2)*a*) du *Code criminel*[161]. L'alinéa 178.11(2)*b*) prévoit un autre cas d'interception légale : lorsque celle-ci est effectuée «en conformité d'une autorisation ...». Le ministère public doit alors prouver non seulement que la police agissait dans le cadre d'une autorisation mais que l'interception de la communication en cause était permise par les modalités de l'autorisation. Au début, les autorisations n'étaient pas toujours rédigées de façon aussi générale qu'elles le sont à l'heure actuelle, et le langage employé n'était pas toujours aussi précis qu'il aurait pu l'être. L'une des premières causes portées en appel fournit un excellent exemple d'interception non effectuée en conformité avec l'autorisation. Dans le jugement *R.* v. *Welsh and Iannuzzi (No. 6)*[162], il a été décidé qu'une interception n'était pas légale lorsque ni l'une ni l'autre des parties à la communication n'étaient nommées ni autrement désignées dans l'autorisation. Le lecteur pourra également consulter l'arrêt *R.* v. *Niles*[163] à ce sujet. D'après ces jugements, le juge devait simplement décider si l'interception effectuée était conforme à l'autorisation.

161. *Goldman* c. *La Reine*, *supra*, note 33.

162. *Supra*, note 31, p. 13-14 (O.R.), p. 375 (C.C.C.).

163. *R.* v. *Niles*, (1978) 40 C.C.C. (2d) 512 (C.A. Ont.).

Toutefois, cette jurisprudence a petit à petit soulevé d'autres problèmes en ce qui concerne la vérification de l'autorisation. Par exemple, lorsque l'autorisation désigne certaines personnes et comporte une clause générale visant des personnes inconnues, que se passe-t-il si un accusé dont le nom n'est pas mentionné dans l'autorisation prétend qu'il était connu des autorités au moment où l'autorisation a été obtenue? Il y a deux façons d'aborder ce problème. D'une part, il ressort de la lecture de l'autorisation que l'accusé n'est pas visé par celle-ci car il n'y est pas désigné expressément et il n'est pas visé par la clause générale. Du moins, c'est l'avis exprimé par la Cour d'appel de l'Ontario dans l'arrêt *R.* v. *Crease (No. 2)*[164]. D'autre part, ce raisonnement semble aussi supposer une vérification de l'autorisation. Afin de déterminer si l'accusé devait être considéré comme une personne inconnue visée par la clause générale, le juge des faits devrait pouvoir prendre connaissance du contenu du paquet scellé pour savoir sur quels renseignements le juge qui a délivré l'autorisation s'est fondé. Apparemment, l'autorisation permet l'interception des communications faites par l'accusé à titre de personne inconnue. Pour l'essentiel, cette solution établit un lien de correspondance entre les personnes inconnues et les personnes non désignées. Ce raisonnement n'est pas tout à fait convaincant, mais il a été accepté par la majorité des juges de la Cour d'appel de la Colombie-Britannique dans l'arrêt *R.* v. *Lloyd and Lloyd*[165]. Il convient de noter que dans l'affaire *Lloyd*, il n'y avait pas d'allégation de fraude ni de non-divulgation.

L'identification des personnes dont les communications seront captées débouche véritablement sur le problème de la vérification de l'autorisation. Par exemple, lorsque l'accusé ne prétend pas simplement qu'il était «connu» au moment de l'obtention de l'autorisation mais que son identité a été délibérément cachée au juge qui a délivré l'autorisation parce que si celui-ci avait été mis au courant de l'intention de la police d'intercepter ses communications (soit en vertu de la clause générale ou à titre de partie à une communication avec une personne nommée dans l'autorisation), l'autorisation n'aurait pas été accordée. Dans l'arrêt *R.* v. *Gill*[166], les preuves obtenues ont été jugées irrecevables après que le juge eut découvert que la police avait dissimulé son intention de capter les communications de la personne non désignée tout en se proposant d'intercepter en prison les conversations entre l'accusé (qui était désigné dans l'autorisation) et la personne non désignée après l'arrestation de l'accusé. La Cour d'appel a décidé que ces conversations n'étaient pas admissibles compte tenu des irrégularités constatées au moment de l'obtention de l'autorisation. Il est intéressant de noter que la Cour a choisi de ne pas se prononcer ni sur la nullité ni sur le caractère exécutoire de l'autorisation, mais plutôt de traiter la question comme un problème d'admissibilité de la preuve. La Cour s'est fondée sur le libellé de l'ancien alinéa 178.16(2)*b*) qui, à l'instar du paragraphe 178.16(3), fait indirectement allusion à la présence de vices de fond (par opposition à des vices de forme) dans la demande d'autorisation.

---

164. *R.* v. *Crease (No. 2)*, (1980) 53 C.C.C. (2d) 378 (C.A. Ont.).

165. *R.* v. *Lloyd and Lloyd*, (1980) 53 C.C.C. (2d) 121 [to C.R. (3d) 221 (C.A. C.-B.), infirmé en partie pour d'autres motifs (1982) 64 C.C.C. (2d) 169, 131 D.L.R. (3d) 112, 39 N.R. 474 (C.S.C.).

166. *Supra*, note 116, p. 176.

La deuxième question, qui soulève clairement le problème de la vérification de l'autorisation, est posée dans l'arrêt *Wilson* c. *La Reine*[167]. Dans cette affaire, le juge des faits, qui avait constaté la présence d'un vice de fond dans la demande en se fondant sur les éléments de preuve produits au procès, a décidé que les conditions de l'alinéa 178.13(1)*b*) n'avaient pas été respectées. Il en est arrivé à cette conclusion après avoir entendu des témoignages de vive voix et sans avoir examiné le contenu du paquet scellé. À l'unanimité, la Cour a jugé que, dans les faits, il avait vérifié l'autorisation et que ce n'était pas la bonne façon de procéder à une révision. Cependant, les avis sont partagés sur la méthode qu'il convenait d'employer. Pour l'essentiel, le jugement de la majorité, rendu par le juge McIntyre, rejette l'approche retenue dans l'affaire *Gill*. La Cour est d'avis que le paragraphe 178.16(3) n'autorise pas le juge à écarter des éléments de preuve en raison de la présence d'un vice de fond lorsque l'interception a été faite conformément à une autorisation apparemment valide. Par voie d'interprétation cependant (et par analogie avec les causes civiles dans lesquelles des ordonnances sont accordées *ex parte*), lorsque l'autorisation a été obtenue irrégulièrement, elle peut être annulée par le juge qui l'a délivrée. Vraisemblablement, toute interception faite en vertu de l'autorisation déclarée par la suite invalide deviendrait rétroactivement illégale, rendant ainsi les communications inadmissibles.

Selon le jugement de la minorité, rendu par le juge Dickson, l'autorisation pourrait être attaquée indirectement par le juge des faits. Toutefois, les juges dissidents étaient d'avis que le juge des faits s'était trompé en décidant qu'il n'avait pas besoin de consulter le contenu du paquet scellé pour déterminer si la demande d'autorisation était entachée d'un vice.

Les deux solutions proposées manquent de souplesse. Exiger que la contestation de l'autorisation ait lieu uniquement devant le juge qui l'a accordée risque de faire perdre beaucoup de temps et d'entraîner la suspension des procès en cours. Même la méthode proposée par le juge Dickson causerait des retards si, comme dans l'affaire *Wilson*, le procès se déroule devant un juge de la cour provinciale qui n'est pas investi du pouvoir d'ouvrir le paquet scellé en vertu de l'article 178.14 du *Code criminel*.

D'autres problèmes sont liés aux motifs de révision ou d'annulation de l'ordonnance, aux conditions devant être remplies, le cas échéant, avant que le paquet scellé ne soit ouvert et, si l'accusé doit prouver la présence d'un vice dans la demande, à la façon dont il pourrait s'acquitter du fardeau sans avoir accès au paquet scellé.

Citant des arrêts rendus en matière civile, le juge McIntyre semble considérer «la fraude ou la découverte de nouveaux éléments de preuve» comme des motifs permettant de faire annuler l'ordonnance rendue *ex parte*. Faisant allusion à la possibilité qu'un autre juge de la même cour soit saisi de la révision de l'ordonnance en raison des exigences de l'administration judiciaire, il déclare : «Le juge chargé de la révision ne doit pas substituer son appréciation à celle du juge qui a accordé l'autorisation. Il n'y a lieu de toucher à l'autorisation que s'il appert que les faits sur lesquels on s'est fondé

167. *Wilson* c. *La Reine*, [1983] 2 R.C.S. 594, 9 C.C.C. (3d) 97.

pour l'accorder diffèrent de ceux prouvés dans le cadre de la révision *ex parte*[168]». On peut se demander d'où proviendront les éléments de preuve nécessaires à l'établissement de ces nouveaux faits. Le jugement de la majorité fait surgir le spectre d'interminables enquêtes préliminaires tenues dans l'espoir de découvrir des faits nouveaux susceptibles de justifier la révision.

Dans son jugement, le juge Dickson n'a pas dressé la liste des motifs de révision, mais il a énuméré les décisions dans lesquelles l'ouverture du paquet scellé a été refusée, sauf s'il y avait une preuve à première vue de fraude ou de non-divulgat... Il a ajouté à ces motifs les déclarations trompeuses. Il semble penser que des raisons justifiant la révision pourraient être révélées pendant le contre-interrogatoire de l'auteur de l'affidavit[169].

Cependant, le spectre d'une perte de temps injustifiée est à nouveau agité. Dans ce genre de régime, les avocats de la défense sont obligés de procéder à l'aveuglette dans l'espoir qu'ils découvriront quelque chose leur permettant de faire ouvrir le paquet scellé, sans même savoir ce qu'ils recherchent.

Le juge Dickson relève enfin un dernier motif de révision, à savoir l'invalidité à première vue de l'autorisation. Par exemple, l'autorisation ne précise pas la période pour laquelle elle sera en vigueur ni la date à laquelle elle a été accordée. Ce sont ces vices, peut-être de forme, que le paragraphe 178.16(3) semble permettre de corriger.

Les problèmes soulevés par la révision, en particulier par la vérification de l'autorisation, sont graves et fondamentaux, tant sur le plan des principes directeurs que sur celui de la procédure. À notre avis, ces problèmes ne pourront être résolus que lorsque les motifs et la procédure à suivre pour la révision et la consultation des documents auront été clairement énoncés.

L'expérience des tribunaux américains en la matière est un peu plus longue et quelque peu différente compte tenu du Title III. Il nous est apparu utile d'examiner les solutions retenues là-bas. Le paragraphe 2518(9) et l'alinéa 2518(1)*a*) du Title III permettent un plus grand accès aux documents que les dispositions de la Partie IV.1 du *Code criminel*. L'alinéa 2518(10)*a*) énonce également des motifs permettant la «suppression» de certains éléments de preuve :

> [TRADUCTION]
> Toute personne lésée dans un procès, une audition ou une procédure tenue devant tout tribunal, ministère, fonctionnaire, organisme, organisme réglementant ou autres services du gouvernement des États-Unis, un État ou une subdivision politique de celui-ci, peut demander la suppression de toutes communications orales ou téléphoniques interceptées ou de toutes preuves en découlant, pour l'un ou l'autre des motifs suivants :

168. *Id.*, p. 608 (R.C.S.), p. 97 (C.C.C.).
169. *Id.*, p. 624 (R.C.S.), p. 112 (C.C.C.).

(i) la communication a été interceptée illégalement;

(ii) l'autorisation ou l'ordonnance permettant l'interception était manifestement insuffisante;

(iii) l'interception n'a pas été effectuée conformément à l'autorisation ou à l'ordonnance[170].

Toute la question de la révision porte véritablement sur le motif énoncé au sous-alinéa (i). Dans l'arrêt *United States* v. *Giordano*[171], la Cour s'est interrogée sur la signification de l'expression [TRADUCTION] «interceptée illégalement» employée au sous-alinéa (i) et a conclu que ces mots ne se rapportaient pas seulement aux amendements à la Constitution car

> [TRADUCTION]
> le Congrès a voulu exiger la suppression d'éléments de preuve lorsque n'ont pas été respectées les exigences législatives qui mettent en œuvre directement et substantiellement son intention de limiter l'usage des procédures d'interception aux seules situations nécessitant le recours à ce dispositif d'enquête extraordinaire[172].

Les arrêts qui ont suivi portaient sur la question de savoir quelles exigences étaient destinées à «mettre en œuvre directement ou substantiellement» l'intention du Congrès ou, en d'autres termes, quelles dispositions [TRADUCTION] «jouaient un rôle de premier plan dans le régime législatif[173]».

Dans son ouvrage intitulé *Wiretapping and Eavesdropping*, C. S. Fishman a dressé une liste des dispositions principales et secondaires qui est reproduite ci-dessous[174] :

> [TRADUCTION]
>
> *Dispositions principales*
>
> 1. FONCTIONNAIRE QUI ACCORDE L'AUTORISATION : 18 USCS par. 2516(1) (gouvernement fédéral) et (2) (État).
> 2. INFRACTIONS DÉSIGNÉES : 18 USCS par. 2516(1) (gouvernement fédéral) et (2) (État).
> 3. CAUSE PROBABLE : 18 USCS sous-alinéas 2518(1)*b*)(i-iii) et alinéas 2518(3) *a*, *b*, *d*).
> 4. MÉTHODES D'INVESTIGATION NORMALES : 18 USCS alinéas 2518(1)*c*) et (3)*c*).
> 5. PÉRIODE MAXIMALE DE TRENTE JOURS : 18 USCS par. 2518(5).
> 6. FIN DE L'AUTORISATION LORSQUE L'OBJECTIF EST ATTEINT : 18 USCS alinéa 2518(4)*e*) et par. 2518(5).
> 7. DEMANDES ANTÉRIEURES : 18 USCS alinéa 2518(1)*e*).

170. Title III, *supra*, note 67, alinéa 2518(10)*a*).

171. *United States* v. *Giordano*, 416 U.S. 505 (1974).

172. *Id.*, p. 527.

173. *Id.*, p. 528.

174. C.S. Fishman, *Wiretapping and Eavesdropping*, Rochester, N.Y., The Lawyers Cooperative Publishing Co., 1978, p. 372-376.

Dispositions secondaires

1. IDENTIFICATION DU FONCTIONNAIRE QUI ACCORDE L'AUTORISATION : 18 USCS alinéas 2518(1)*a*) et (4)*d*).
2. IDENTIFICATION DES PERSONNES VISÉES PAR LA DEMANDE : 18 USCS sous-alinéa 2518(1)*b*)(iv).
3. IDENTIFICATION DES PERSONNES VISÉES PAR LE MANDAT : 18 USCS alinéa 2518(4)*a*).
4. ÉTAT ET NOTIFICATION : 18 USCS alinéa 2518(8)*d*).

Les dispositions principales (3) et (4) ainsi que les dispositions secondaires (2) et (3) nécessitent un examen plus minutieux car ces motifs pourraient être invoqués, ou l'ont été, en vertu de la législation canadienne. En la matière, l'arrêt *United States* v. *Donovan*[175] fait autorité. Il a été décidé

> [TRADUCTION]
> qu'une demande d'autorisation d'écoute clandestine devait désigner nommément une personne si le gouvernement est fondé à croire que celle-ci participe à l'activité criminelle qui fait l'objet de l'enquête et espère pouvoir intercepter ses conversations grâce à la mise sur écoute de son poste téléphonique[176].

Cette opinion avait été exprimée antérieurement dans l'arrêt *United States* v. *Kahn*[177].

Il a été décidé que le sous-alinéa 2518(10)*a*)(i) n'exigeait pas la suppression des conversations de Donovan. La Cour a choisi une approche quelque peu pratique et s'est demandée si le juge qui avait accordé l'autorisation aurait agi différemment[178].

L'argumentation de l'affaire *Donovan* démontre que les éléments de preuve seraient supprimés si les autorités n'avaient aucun motif de croire que les méthodes d'investigation normales auraient été infructueuses. Évidemment, si le juge saisi d'une demande en application de l'alinéa 2518(3)*c*) sait que des méthodes d'enquête normales ont été appliquées avec succès, il n'a pas le pouvoir d'accorder le mandat. Du reste, les exigences du paragraphe 2518(3), comme celles du paragraphe 178.13(1) du *Code*, témoignent de l'intention du Congrès (ou du Parlement) de limiter le recours à cette méthode d'enquête extraordinaire, source d'importante immixtion dans la vie privée.

Il est certain que l'approche retenue dans l'affaire *Donovan* suffit pour confirmer le principe de la modération. Qu'en est-il alors du respect de la vie privée? Nous pensons que l'approche choisie contribuera probablement à faire valoir le droit à l'intimité de la vie privée. En revanche, tout le débat sur l'identification des personnes visées par

175. *Supra*, note 117.

176. *Id.*, p. 428.

177. *United States* v. *Kahn*, 415 U.S. 143 (1974), p. 155. La Cour a alors rejeté l'exigence selon laquelle l'ordonnance devait désigner toutes les personnes que le gouvernement aurait pu découvrir à la suite d'une enquête diligente.

178. *Supra*, note 117, p. 435.

l'autorisation ne soutient pas vraiment le droit à la vie privée, sauf dans les cas où l'on peut dire que le juge n'aurait pas accordé l'autorisation ou n'aurait pas pu le faire s'il avait su qui elle visait véritablement (*Gill*[179]) ou s'il avait su qu'il y aurait peut-être interception sans discrimination des communications privées de personnes inconnues. À notre avis, ce dernier problème concerne la restriction de l'interception des communications privées, laquelle peut souvent comporter des distinctions très ténues. Lorsqu'il est manifeste que l'autorisation serait accordée à l'égard des principales personnes visées, on ne peut guère assurer la protection de l'intimité personnelle en exigeant que la police *désigne* dans l'autorisation des personnes qui peuvent être impliquées dans l'enquête de façon seulement accessoire, sous peine d'annulation de l'autorisation. Cette mesure aura simplement pour effet d'élargir le champ d'application de l'enquête plutôt que de le restreindre. Lorsque la personne manifestement visée n'est pas identifiée, l'on pourra conclure à l'existence d'une dissimulation et régler ce problème grâce à un raisonnement du genre de celui qui a été retenu dans l'affaire *Gill*.

Comme le lecteur le sait déjà, l'alinéa 2518(10)*a*) du Title III prévoit un troisième motif pour la suppression des éléments de preuve, celui de l'interception qui n'a pas été effectuée conformément à l'ordonnance ou à l'autorisation. L'alinéa 178.16(1)*a*) du *Code criminel* a été interprété de façon similaire, et cela ne pose aucun problème nouveau.

Depuis l'affaire *Wilson*, quelques décisions ont été rendues par des juges ayant accordé une autorisation à qui l'on demandait d'annuler leur ordonnance. Jusqu'ici, aucun principe rigoureux n'a été énoncé en ce qui concerne l'ouverture du paquet ou l'annulation de l'ordonnance par le juge. Dans l'arrêt *R.* v. *Delhaye*[180], il semble que le juge O'Leary ait ouvert le paquet et annulé l'ordonnance pour la simple raison que l'affidavit ne désignait pas deux des parties dont les communications privées devaient être interceptées du fait que l'on avait des motifs raisonnables et probables de croire que cette interception pourrait être utile à l'enquête. Il semble que cette solution soit draconienne. D'après les motifs du jugement, il ne semble pas que cette omission ait été faite de mauvaise foi (comme dans l'affaire *Gill*). Le juge n'explique pas non plus pourquoi toute l'ordonnance est annulée. Il est important de souligner que le juge O'Leary ne s'est pas demandé s'il aurait accordé l'ordonnance a) s'il avait été mis au courant de tous les faits; b) si, en plus, on lui avait révélé l'identité des deux personnes visées; c) si on lui avait au contraire caché l'identité des deux personnes visées; d) s'il n'avait pas été mis au courant des faits du tout. Cette décision s'explique peut-être par le fait qu'aucun principe n'est énoncé dans l'affaire *Wilson*[181] en ce qui concerne les cas où l'autorisation peut être annulée, si l'on fait exception du commentaire peu utile du juge McIntyre, que nous avons rapporté ci-dessus, et qui avait été inspiré par les arrêts portant sur l'annulation des ordonnances *ex parte* en matière civile.

179. *Supra*, note 116.

180. *R.* v. *Delhaye*, Haute cour de l'Ontario, 7 mars 1984 (le juge O'Leary), jugement non publié.

181. *Supra*, note 167.

Dans une autre décision rendue après l'affaire *Wilson*, un autre problème d'ordre pratique est soulevé par la procédure retenue dans cet arrêt. Dans la décision *R.* v. *Con and Fung*[182], le juge Huddart de la Cour de comté, qui avait accordé l'autorisation a dû statuer, sur la foi des témoignages produits au cours d'autres poursuites, sur l'étendue des connaissances de la police en ce qui concerne l'identité de l'un des auteurs du complot et sur la possibilité d'avoir recours à d'autres techniques d'enquête ordinaires. Certains éléments de preuve étaient incompatibles et le juge a dû se prononcer sur la crédibilité des témoins. Il a fait remarquer qu'il lui était [TRADUCTION] «très difficile d'apprécier la déposition de l'agent chargé de l'enquête». Le juge Huddart a également dû trancher une autre question épineuse, à savoir dans quelles circonstances pouvait-il ouvrir le paquet s'il était allégué qu'au moins l'une des conditions énoncées à l'alinéa 178.13(1)*b*) n'avait pas été respectée. Il a conclu que ce motif n'était pas suffisant car il devait y avoir une preuve *prima facie* d'un manquement aux trois conditions avant que le paquet scellé puisse être ouvert, ou encore, il devait y avoir des preuves d'une duperie délibérée relative à l'une des conditions. Le fait que l'une d'entre elles n'avait pas été respectée ne suffisait pas[183].

C. Le secret

La question de l'accès aux documents est liée de très près au problème de la révision. L'article 178.14 du *Code criminel* contient des dispositions assez exceptionnelles visant à tenir secrets les documents produits lors de la demande; ceux-ci sont placés dans un paquet scellé qui doit être gardé par le tribunal et qui ne peut être ouvert que pour statuer sur une demande de renouvellement de l'autorisation ou qu'en application d'une ordonnance d'un juge visé à cet article[184].

Même si en vertu du sous-alinéa 178.14(1)*a*)(ii), un juge défini à l'article 482 est habilité à ouvrir le paquet scellé, ce pouvoir est interprété de façon très stricte. La décision rendue par le juge Krever dans l'affaire *Re Stewart and The Queen*[185] illustre bien cette interprétation : le juge a statué que le pouvoir d'ouvrir le paquet scellé [TRADUCTION] «est un pouvoir qui doit être limité aux cas exceptionnels[186]» et que ce n'est que [TRADUCTION] «très rarement[187]» que ce pouvoir est exercé.

Le juge Krever ne précise pas les motifs qui *justifieraient* une ordonnance visée au sous-alinéa 178.14(1)*a*)(ii); d'autres affaires, comme la décision *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*[188], limitent cependant les circonstances à la fraude et à des méfaits semblables de la part des autorités.

182. *R.* v. *Con and Fung*, (1984) 11 C.C.C. (3d) 396 (Cour de comté C.-B.).

183. *Id.*, p. 404.

184. *Code criminel*, par. 178.14(1).

185. *Re Stewart and The Queen*, (1976) 30 C.C.C. (2d) 391 (Haute cour Ont.).

186. *Id.*, p. 401.

187. *Id.*, p. 402.

188. *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*, (1978) 40 C.C.C. (2d) 212 (C.S. Alb.), p. 219.

L'article 178.14 constitue aussi un obstacle pour la personne qui a fait l'objet d'une interception et qui en a été avisée, en vertu de l'article 178.23, mais qui n'a pas été poursuivie. Cette personne est pratiquement privée de toute possibilité de contester la légalité de l'interception autorisée, en raison des dispositions en matière de secret[189].

Les motifs permettant l'ouverture du paquet s'apparentent aux motifs justifiant la révision de l'autorisation dans les affaires entendues avant l'arrêt *Wilson*. Comme le juge Zuber l'a indiqué dans l'affaire *R.* v. *Welsh and Iannuzzi (No. 6)*[190], de tels motifs [TRADUCTION] «comprendraient des cas où l'autorisation était manifestement irrégulière, ou entachée d'un vice du fait de son obtention frauduleuse[191]».

Une autorisation ne peut être cassée que s'il y a fraude ou non-divulgation volontaire. Pour être en mesure de prouver la fraude ou la non-divulgation, la défense doit avoir accès au paquet scellé, mais il lui faut au préalable montrer qu'il y a eu fraude ou non-divulgation. C'est un cercle que certains avocats ont tenté de briser en contre-interrogeant l'agent de police qui a rédigé l'affidavit. Les tribunaux n'ont pas tardé à déceler l'illogisme de cette tactique. Ainsi, dans l'affaire *R.* v. *Haslam*[192], le tribunal a jugé que l'agent ne pouvait être contre-interrogé à l'égard du contenu de l'affidavit en l'absence d'une ordonnance prévue à l'article 178.14. Outre la question de la révision, à laquelle nous reviendrons, les dispositions en matière de secret soulèvent d'autres problèmes :

a) les données pratiques sont limitées en ce qui a trait à l'étendue des clauses générales;

b) il n'y a pratiquement aucune donnée sur l'existence, dans les faits, des exigences préalables prévues par la loi — par exemple, que d'autres méthodes d'enquête ont été utilisées et ont échoué;

c) il n'y a pratiquement aucune donnée sur le recours, dans les faits, à des clauses générales pour les interceptions;

d) il n'y a pratiquement aucune donnée sur le monitorage des dispositifs;

e) il n'existe pratiquement aucun moyen de déterminer la gravité de l'affaire qui a donné lieu aux interceptions.

Il s'agit fondamentalement de problèmes de transparence et de responsabilité, et la position de la Commission de réforme du droit est de favoriser dans la mesure du possible la transparence et la révision des actes accomplis par les forces de l'ordre. Dans l'arrêt *MacIntyre*[193], le juge Dickson s'est clairement prononcé en faveur de la «transparence» des actes judiciaires en matière de mandat de perquisition; le même argument peut également s'appliquer aux autres champs des pouvoirs de la police.

189. *Re Zaduk and The Queen*, (1979) 46 C.C.C. (2d) 327 (C.A. Ont.). Ce problème est étudié plus loin, sous la rubrique «VI. B. L'avis en vertu de l'article 178.23».

190. *Supra*, note 31.

191. *Id.*, p. 371-372.

192. *R.* v. *Haslam*, (1977) 36 C.C.C. (2d) 250 (C. Dist. T.-N.).

193. *Supra*, note 96.

Le juge Dickson déclare que la préoccupation de responsabilité n'est pas entamée par le fait que les mandats de perquisition peuvent être délivrés par un juge de paix à huis clos; au contraire, ce fait «donne du poids à la thèse en faveur de la politique d'accessibilité». Il précise ce qui suit : «ce qu'il faut viser, c'est le maximum de responsabilité et d'accessibilité, sans aller jusqu'à causer un tort à un innocent ou à réduire l'efficacité du mandat de perquisition comme arme dans la lutte continue de la société contre le crime». Il conclut par la suite que «restreindre l'accès du public ne peut se justifier que s'il est nécessaire de protéger des valeurs sociales qui ont préséance. C'est notamment le cas de la protection de l'innocent[194]».

Il s'agit de savoir si en matière de surveillance électronique, le secret est nécessaire pour «protéger des valeurs sociales qui ont préséance». Les représentants de la police et de l'État ont identifié deux valeurs : la protection des informateurs et la protection des techniques d'investigation de la police. On nous a également fait valoir que le système actuel de secret encourage les responsables à faire preuve d'une plus grande franchise dans la production des documents devant le juge appelé à donner l'autorisation et que dans l'éventualité d'un régime plus ouvert, les policiers et les agents seraient vraisemblablement moins enclins à présenter la totalité des éléments devant le juge appelé à trancher. Cette question est importante lorsque la *seule* méthode pour assurer la responsabilité se limite à l'approbation judiciaire préalable. Elle est moins importante lorqu'il existe des procédures de révision postérieure à l'interception. Sans chercher à minimiser l'importance de cette préoccupation, il faut toutefois reconnaître qu'elle peut être quelque peu exagérée, comme en fait foi l'expérience de la commission McDonald[195].

Quelles sont donc les valeurs de la société qui militent en faveur de l'interprétation adverse?

1. *La modération* : la proportion très élevée des autorisations accordées, en comparaison de la situation qui prévaut aux États-Unis, donne à penser que l'on demande des autorisations dans des circonstances où les infractions visées par les enquêtes ne sont pas graves et où d'autres méthodes d'enquête seraient plus appropriées — on observe donc une généralisation injustifiée d'un moyen très attentatoire.

2. *La responsabilité* : une fois l'autorisation accordée, il n'y a essentiellement aucune vérification de la véracité des documents déposés lors de la demande.

3. *La révision* : l'accusé n'a pratiquement aucune possibilité de mettre en cause la légalité de la demande.

4. Les personnes visées mais non accusées ne peuvent mettre en cause la légalité de la demande et de l'interception devant les tribunaux civils.

194. *Id.*, p. 183-187 (R.C.S.), p. 144-147 (C.C.C.).

195. *Supra*, note 125, vol. 2, p. 1080-1081.

D. Conclusion

Comme nous l'avons indiqué plus haut, les problèmes de la révision et du secret sont liés de très près, et toute solution aux questions de révision est fonction du degré d'accessibilité des documents. On nous a par conséquent proposé d'adopter une procédure en vertu de laquelle l'accusé aurait plein accès aux documents produits lors de la demande, comme cela se fait aux États-Unis. Nous avons interrogé nos experts-conseils sur la viabilité de cette procédure, et de façon quasi unanime, sous réserve d'une méthode assurant la protection de l'identité des informateurs et des personnes qui viennent en aide à la police, on estime qu'il n'existe aucune raison de ne pas donner accès plein et entier à la défense. Les personnes consultées ont affirmé clairement ne voir aucun problème grave en termes de divulgation des techniques d'investigation de la police. Elles ne prévoient aucun effet négatif important sur la qualité des documents qui doivent être produits lors de la demande. En dépit de la crainte que le nom des suspects qui ne sont pas accusés puisse être divulgué, on juge que les problèmes sont amplement compensés par les gains en matière de responsabilité et même d'efficacité judiciaire. Nous avons déjà souligné qu'en vertu du régime actuel, l'identité des personnes nommées dans une autorisation est divulguée lors du procès même si certaines de ces personnes n'ont pas fait l'objet d'une accusation. Un autre problème soulevé est celui du risque que la divulgation nuise à d'autres enquêtes connexes en cours. Il existe cependant un consensus sur le fait que cela constituerait très rarement un problème et que si le cas se posait, le ministère public aurait alors tout simplement à prendre une décision sur l'opportunité et le moment d'intenter des poursuites. Il s'agit là d'un problème qui n'est pas particulier à la surveillance électronique, et à l'égard duquel il n'y a par conséquent pas lieu d'instituer une règle spéciale. Le problème des informateurs de la police est différent. Ceux-ci ont toujours bénéficié d'un statut particulier et d'une protection spéciale qui ont été confirmés de façon très explicite et presque absolue par la Cour suprême du Canada[196]. Il existe une possibilité réelle de danger pour l'informateur en cas de divulgation de son identité. La solution adoptée aux États-Unis consiste à rédiger les documents produits avec la demande de façon à cacher l'identité de l'informateur. Nous proposons une méthode plus directe permettant de demander à un juge, par requête *ex parte*, de sceller ou de rayer des parties de la déclaration assermentée.

Enfin, on nous a fait part d'inquiétudes au sujet de la divulgation de l'identité de personnes qui, sans être de vrais informateurs, consentent à aider la police en échange d'une promesse d'anonymat. Tel est le cas d'un propriétaire qui permettrait à la police d'utiliser sa maison comme point de surveillance. On a fait valoir qu'en certains cas il peut s'avérer nécessaire de révéler l'identité de cette personne dans l'affidavit afin d'obtenir l'autorisation, mais qu'il n'existe aucun intérêt réel à la divulguer publiquement. Puisque ces cas s'apparentent globalement aux cas des informateurs de la police, nous pensons qu'ils peuvent être compris dans la procédure consistant à sceller une

196. Voir, par exemple, *Bisaillon* c. *Keable*, [1983] 2 R.C.S. 60, 7 C.C.C. (3d) 385, 2 D.L.R. (4th) 193 et *Le solliciteur général du Canada* c. *La Commission royale d'enquête sur la confidentialité des dossiers de santé en Ontario*, [1981] 2 R.C.S. 494, 62 C.C.C. (2d) 193.

partie des documents. Il s'agit alors de déterminer quand et comment la révision de l'autorisation doit avoir lieu, et quelles sont les conséquences de cette révision. La demande fondée sur l'arrêt *Wilson*[197] semble être absolument insatisfaisante. Elle peut entraîner d'importants délais et retards et nuire au bon déroulement du processus judiciaire. Puisque la question de la révision de l'autorisation est liée à la recevabilité de la preuve, elle devrait être tranchée lors du procès ou de l'enquête préliminaire, selon le cas. De façon générale, il existe deux catégories de motifs de révision du processus de demande : l'erreur et la fraude.

Par «erreur», nous entendons l'erreur que commet le juge en accordant une autorisation alors qu'à première vue, la demande ne contient pas suffisamment de motifs sur lesquels rendre une ordonnance. Par «fraude», nous visons le cas où, même si la demande et l'affidavit sont valides à première vue, on peut prouver que les faits ne correspondent pas à l'affidavit ou qu'il y a eu omission volontaire de faits pertinents. Théoriquement, l'un ou l'autre de ces motifs pourrait nous permettre de décider qu'il y a eu, dans la procédure de demande, un défaut qui appelle une sanction. Il faut cependant nous demander si l'irrecevabilité de la preuve est la sanction appropriée dans les deux cas. Pour les raisons que nous présenterons plus loin, sous la rubrique «Les recours», nous jugeons que seule la catégorie de la fraude constitue une base suffisante pour l'exclusion de la preuve. Il s'ensuit donc que la révision du processus de demande doit se limiter à ces motifs. Il se peut que la personne visée dispose d'autres recours au civil ou que l'on doive en établir d'autres dans les cas où une autorisation est accordée par erreur pour un motif insuffisant. Cette question mise à part, nous aimerions qu'un groupe d'experts puisse réviser les autorisations après un certain nombre d'années afin de vérifier l'observation des dispositions des articles 178.12 et 178.13. Avec des dispositions de divulgation plus libérales, une telle révision serait désormais possible.

Si l'on accepte le principe de l'irrecevabilité de la preuve en cas de défaut de fond dans la demande, selon la définition qui sera donnée plus loin (c'est-à-dire lorsqu'il y a fraude), alors ces points deviennent uniquement une question de procédure.

(1) Premier point : À quel moment la question est-elle étudiée?

Une des critiques les plus fréquentes de la législation relative à l'écoute électronique porte sur la longueur des procédures de voir-dire nécessaires pour trancher les questions de recevabilité. Aussi importe-t-il, dans la mesure du possible, de ne pas ajouter considérablement à la longueur et à la multiplicité des procédures. D'autre part, nous pensons qu'il arrivera rarement qu'il faille tenir une audience sur la preuve pour trancher ces questions en raison de la définition du vice de fond de la demande. Une décision lors de l'enquête préliminaire peut sembler une perte de temps. La décision ne lie pas les parties dans les procédures subséquentes[198]. Par contre, l'accusé a le droit d'assurer

197. *Supra*, note 167.

198. *R.* c. *Duhamel*, [1984] 2 R.C.S. 555, 57 N.R. 162.

sa pleine défense à l'étape de l'enquête préliminaire et, par tradition, ce sont les mêmes règles de preuve qu'au procès qui s'appliquent alors[199]. Un accusé pourrait avec raison prétendre qu'il ne devrait pas être forcé d'assumer les dépenses et les inconvénients d'un procès si la seule preuve qui est retenue contre lui est irrecevable. Il s'agit là d'arguments très logiques, et il faut faire un choix politique. Comme nous sommes d'avis que l'audition nécessaire ne devrait pas prolonger indûment les procédures, nous avons choisi de permettre la contestation de la procédure de demande à l'étape de l'enquête préliminaire tout comme à celle du procès.

(2) Deuxième point : Comment la question est-elle résolue?

En vertu du projet de modification de l'article 178.14, l'accusé aura accès à presque tous les documents présentés au moment de la demande. Il pourra alors étudier les documents avec ses conseillers juridiques et, après avoir effectué les recherches qu'il jugera appropriées, il sera en mesure d'estimer s'il existe un fondement pour contester le document sur la base d'une fraude ou d'une conduite insouciante de la part des autorités (le critère de l'irrecevabilité établi à la recommandation 63). À notre avis, il incombe à l'accusé de soulever au moins la question d'un vice de fond avant d'avoir le droit de demander une audition sur la preuve au cours de laquelle les agents de police pourraient être appelés à témoigner. Nous pensons que le fondement d'une audition portant sur la preuve pourrait être présenté dans un document fait sous serment qui ne serait cependant pas recevable contre l'accusé au moment du procès lui-même[200]. Le juge pourrait être tenu de déterminer s'il existe une base suffisante pour décréter une audition portant sur la preuve. Il va sans dire que si le document de l'affidavit ne révèle que des inexactitudes de peu d'importance, qui ne peuvent aucunement mettre en cause l'intégrité de la procédure de demande, il n'existe alors aucun fondement pour décréter une audition plus approfondie.

Cependant, lorsque les documents soulèvent réellement une question quant à la possibilité d'un vice de fond dans la demande, alors le juge doit décréter une audition complète. En raison de la nature des motifs de recevabilité, nous croyons qu'il incombe au ministère public de démontrer l'intégrité du processus de la demande. Il aura plein accès aux documents et au personnel en cause, et il est en meilleure position pour présenter la preuve permettant de trancher adéquatement ces questions[201].

---

199. *R.* v. *Pickett*, (1975) 28 C.C.C. (2d) 297 (C.A. Ont.); *Re Stillo and The Queen*, (1981) 60 C.C.C. (2d) 243 (C.A. Ont.).

200. Une règle comparable semble s'appliquer à l'égard du témoignage de l'accusé au cours d'un voir-dire. Voir *Erven* c. *La Reine*, [1979] 1 R.C.S. 926, (1978) 44 C.C.C. (2d) 76.

201. La procédure suggérée est semblable à la procédure comparable en vigueur aux États-Unis; voir J.G. Carr, *op. cit. supra*, note 67, p. 349-350; *Franks* v. *Delaware*, 438 U.S. 154 (1978); *United States* v. *Licavoli*, 604 F.2d 613 (1979) (9th Cir.).

RECOMMANDATIONS

48. L'article 178.14 du *Code criminel* devrait être modifié pour inclure ce qui suit :

a) en plus des exceptions prévues à l'alinéa (1)*a*), donner accès aux documents du paquet scellé afin de permettre d'examiner une demande d'autorisation relative à des enquêtes connexes;

b) permettre au mandataire spécialement désigné de conserver une copie conforme de tous les documents relatifs à la demande faite en vertu de l'article 178.12 ou du paragraphe 178.13(3).

49. Lorsqu'il donne le préavis prévu au paragraphe 178.16(4), le ministère public inclut une copie de l'autorisation et des renouvellements en vertu desquels les interceptions ont eu lieu, et sous réserve d'une ordonnance de la Cour, une copie de tous les documents relatifs à une demande d'autorisation ou de renouvellement.

50. Avant de donner le préavis prévu au paragraphe 178.16(4), le mandataire spécialement désigné peut, dans une requête *ex parte* et hors cour, demander à un juge défini à l'article 482 du *Code criminel* d'émettre une ordonnance de non-divulgation de certaines parties des documents pour le motif que leur divulgation risque d'entraîner la révélation de l'identité de l'informateur ou de celle de toute personne ayant collaboré à l'enquête; dans ce dernier cas, il faut montrer que la non-divulgation de l'identité de ces personnes ne nuit pas à l'intérêt public. La demande doit être faite par écrit et être accompagnée de l'affidavit de l'agent de la paix.

51. La personne contre qui l'on cherche à faire admettre une preuve en vertu de l'alinéa 178.16(1)*a*) du *Code criminel* à la suite d'une interception effectuée en vertu d'une autorisation ou d'un renouvellement, peut demander lors de l'enquête préliminaire ou du procès, que la preuve ou la preuve dérivée soient exclues en raison d'un vice de fond dans la demande d'autorisation ou de renouvellement. La procédure suivante devrait s'appliquer :

a) la demande devrait être faite par écrit et être accompagnée d'un affidavit (ou d'une preuve donnée de vive voix avec la permission du juge);

b) le juge ne doit tenir une enquête sur la validité de la demande d'autorisation ou de renouvellement que si la demande et la preuve y afférente, de même que les documents divulgués en vertu de la recommandation 49, soulèvent réellement, à l'égard de la demande, la question d'un vice de fond, au sens de la recommandation 62, qui pourrait entraîner l'exclusion de la preuve;

c) lorsque le juge ordonne une enquête, il incombe au ministère public de prouver au tribunal que la demande n'est entachée d'aucun vice de fond au sens de la recommandation 62;

d) l'affidavit et le témoignage de l'accusé ne peuvent être invoqués par le ministère public à l'étape de l'enquête préliminaire ou du procès.

IV. L'autorisation en cas d'urgence : l'article 178.15

À l'égard de la procédure d'autorisation en cas d'urgence, on a porté à notre attention le problème de la victime d'enlèvement. Certains organismes chargés de l'application de la loi désirent apparemment être en mesure de procéder à une surveillance électronique dès qu'ils parviennent à localiser la victime, sans être tenus d'invoquer la procédure d'urgence prévue à l'article 178.15. Certains suggèrent de légaliser de telles interceptions en présumant que la victime de l'infraction a donné son consentement à toute interception. En gros, nous ne voyons pas comment cela améliorerait la situation, puisqu'il est fort peu probable que la victime participe à bon nombre de conversations. L'interception de communications destinées à la personne qui fait l'objet de chantage ou d'extorsion serait déjà légale si elle était faite avec le consentement de cette personne. Dans la seule décision publiée qui étudie cette question, soit *R.* v. *Gamble and Nichols*[202], il semble que la police a eu le temps d'obtenir cette autorisation (qui a cependant été jugée inadéquate)[203]. À notre avis, il suffirait d'une légère modification de l'article 178.15 pour donner une longueur d'avance à la police dans ces situations dangereuses.

Une autre lacune de l'article 178.15 est l'absence d'un relevé des procédures. Même si le paragraphe 178.15(2) exige que l'autorisation soit donnée par écrit, aucune disposition ne prévoit que la demande doit être faite par écrit. Par conséquent, il est pratiquement impossible de réviser la demande par la suite. À notre avis, surtout à la lumière de nos recommandations en matière de divulgation, il est souhaitable qu'il existe un registre des demandes; à cette fin, il nous semble que la procédure proposée pour le télémandat à l'article 70 du projet de loi C-18, qui ajouterait l'article 443.1 au *Code criminel*, serait le mécanisme le plus simple et le plus efficace pour consigner les faits sur lesquels le juge s'est fondé pour accorder l'autorisation. Les faits qui devraient être consignés seraient les raisons justifiant la procédure d'urgence, les motifs pour demander l'autorisation d'intercepter, de même que le nom des personnes visées et les lieux de l'interception. Il s'agit là, selon nous, de l'ensemble minimal des éléments qui doivent être consignés.

RECOMMANDATIONS

52. L'article 178.15 devrait être modifié par l'adjonction du paragraphe (6) suivant :

> **La recevabilité de la preuve obtenue à la suite d'une ordonnance délivrée en vertu du présent article n'est pas entachée par le fait que le dispositif électromagnétique, acoustique, mécanique ou autre a été installé avant l'obtention de l'ordonnance, lorsque l'ordonnance rendue en vertu du présent article a**

202. *R.* v. *Gamble and Nichols*, (1978) 40 C.C.C. (2d) 415 (D.A., C.S. Alb.).
203. *Id.*, p. 423-424.

été obtenue à l'égard d'une infraction visée par le paragraphe 247(1) (enlèvement) et qu'aucune communication privée n'a été obtenue au moyen de ce dispositif avant l'obtention de l'ordonnance.

53. Une demande d'autorisation en cas d'urgence en vertu de l'article 178.15 devrait obligatoirement être faite par écrit, par téléphone ou par d'autres moyens de télécommunication, et il devrait y avoir consignation des faits, notamment : une déclaration des motifs pour lesquels l'autorisation ne pouvait, avec une diligence raisonnable, être obtenue en vertu de l'article 178.13; les faits justifiant l'obtention d'une autorisation, de même que les faits particuliers de l'infraction; le nom des personnes dont on cherche à intercepter les communications privées ainsi que les lieux de l'interception.

V. Les recours

A. La recevabilité de la preuve relative à d'autres infractions

La nature de la surveillance électronique est telle qu'il est possible que la preuve d'autres infractions que celles qui sont énoncées dans l'autorisation puisse être obtenue par interception. C'est tout particulièrement le cas dans un système qui n'exige pas que l'on réduise au minimum les sujets de conversation pouvant faire l'objet de l'écoute électronique. Cet état de fait soulève les questions suivantes :

1. La loi devrait-elle faire une distinction entre la preuve inattendue et la preuve qui pouvait être prévue?

2. Dans l'un et l'autre cas, avons-nous besoin d'un système pour l'obtention d'une autorisation relativement aux nouvelles ou aux autres infractions?

3. Comment devons-nous traiter la recevabilité d'une telle preuve?

4. Comment devons-nous traiter la preuve d'infractions pour lesquelles aucune autorisation n'aurait pu être obtenue?

Il convient d'aborder en premier lieu la question de la preuve inattendue. On peut faire une analogie avec la fouille, la perquisition et la saisie, où l'on accepte généralement que la preuve est saisie légalement (sous l'angle constitutionnel) lorsqu'elle est trouvée au cours d'une perquisition légale visant d'autres preuves dans des circonstances où la découverte de nouvelles preuves n'était pas prévue. Il s'agit tout simplement d'une application de ce qu'on appelle la doctrine des choses en vue, dans la jurisprudence fondée sur le quatrième amendement des États-Unis[204].

204. *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971); *Texas* v. *Brown*, 103 S.Ct. 1535 (1983); la doctrine est reconnue en common law : *Chic Fashions (West Wales) Ltd.* v. *Jones*, [1968] 2 Q.B. 299 (C.A.).

Lorsque la preuve est imprévue, aucun problème sérieux ne se pose. L'intimité de la vie privée n'est pas menacée gravement puisque l'intrusion dans la vie privée a déjà été autorisée, de façon légitime, pour d'autres raisons.

L'intégrité du mécanisme prévu par la loi n'est pas non plus mise en danger lorsqu'on permet aux autorités d'utiliser cette preuve. Au contraire, le refus d'utiliser une telle preuve pourrait entraîner de sérieuses conséquences sur la perception de la légitimité du mécanisme, comme l'indique l'affaire *United States* v. *Cox*[205].

Les questions de politique surgissent lorsque la preuve d'autres infractions est prévue. En pareil cas, la protection de la vie privée est en cause et l'intégrité du mécanisme prévu par la loi est menacée. Le fondement sous-jacent à la législation sur l'écoute électronique est l'acceptation à regret du fait qu'en certaines circonstances clairement définies, des atteintes graves à la vie privée peuvent être admises. Au fond, le mécanisme prévoit que de telles atteintes sérieuses ne sont permises que pour l'enquête relative à certaines infractions. Théoriquement, les infractions à l'égard desquelles il est permis de pratiquer l'écoute électronique ont été retenues à la suite d'un grand effort d'équilibrage des intérêts en jeu. Le fondement de tout le mécanisme est mis en danger si une autorisation est obtenue à l'égard d'une infraction de façon à couvrir d'autres infractions qui peuvent ou non faire l'objet d'une demande d'autorisation (interceptions subreptices).

Le premier contrôle dans ce domaine doit se faire soit par la surveillance judiciaire, au moment de la procédure de demande, soit par l'examen de la recevabilité de la preuve. Malheureusement, rien ne laisse croire que le contrôle nécessaire puisse être exercé à l'étape de la demande d'autorisation. Par conséquent, nous croyons que la procédure de demande devrait être établie de façon que le contrôle puisse être exercé à l'étape de la recevabilité de la preuve. À notre avis, la seule façon efficace de prévenir les interceptions subreptices consiste à exiger la preuve de la bonne foi au moyen d'un voir-dire durant le procès chaque fois qu'une partie cherche à introduire la preuve d'infractions qui ne sont pas décrites dans l'autorisation. Ce fardeau supplémentaire qui incombe au ministère public encouragera la divulgation complète à l'étape de la demande, puisqu'il constituera alors une incitation à obtenir une autorisation décrivant toutes les infractions pour lesquelles une autorisation pourrait être obtenue. Cela découragera également les tentatives d'obtenir des autorisations comme moyen détourné d'acquérir la preuve d'autres infractions pour lesquelles des autorisations ne peuvent être demandées. À notre avis, la bonne foi dans ce contexte comprendrait notamment les conditions suivantes :

a) Au moment de la demande d'autorisation ou de renouvellement, il était raisonnablement impossible de prévoir l'obtention de preuves relatives à des infractions non désignées dans la demande.

b) Si l'on prévoyait obtenir des éléments de preuve relatifs à d'autres infractions, celles-ci n'ont pas été désignées dans la demande parce qu'il ne s'agissait pas

205. *United States* v. *Cox*, 449 F.2d 679 (1971) (10th Cir.), p. 686-687.

d'infractions susceptibles de donner lieu à une autorisation *et* qu'elles ne formaient pas l'objet principal de l'enquête, mais n'étaient *qu'indirectement reliées* à l'enquête sur les infractions désignées dans l'autorisation.

c) Au moment de la demande ou du renouvellement, on a déclaré au juge à quelles autorités l'on entendait remettre les renseignements obtenus grâce à l'interception. (Cela pourrait fournir un indice important des vrais motifs et de la bonne foi des autorités. Ainsi, le fait de révéler au juge que l'on cherche à transmettre l'information aux autorités fiscales pourrait apporter un éclairage sur l'objectif réel de l'enquête[206].)

d) Lorsque les éléments de preuve concernent une infraction à l'égard de laquelle il était possible d'obtenir une autorisation, et si l'on croyait possible d'obtenir des preuves de cette infraction, cette croyance a été divulguée dans les documents présentés à l'appui de la demande *et* l'infraction n'a pas été désignée dans l'autorisation pour les seules raisons suivantes : (i) les soupçons n'étaient pas suffisants pour satisfaire au critère prévu par la loi; (ii) l'enquête sur l'infraction ne constituait pas le but principal de l'enquête, mais n'en était *qu'un but secondaire*.

À notre avis, il s'agit de garanties raisonnables qui ne se démarquent pas de l'arrêt *R.* c. *Commisso* de la Cour suprême du Canada[207]. Bien que cette affaire ait porté principalement sur l'interprétation du paragraphe 178.16(3.1) du *Code criminel*, tous les juges ont traité de la question de la bonne foi. Dans son opinion dissidente, le juge Dickson affirme qu'une autorisation serait obtenue de mauvaise foi «si la police, bien qu'enquêtant aussi bien sur l'infraction qui est spécifiée que sur celle qui ne l'est pas, s'intéressait principalement à l'infraction non spécifiée à l'égard de laquelle elle ne pourrait obtenir une autorisation[208]».

À notre avis, la dérogation aux normes de la bonne foi établies par la loi peut être considérée comme un motif d'exclusion de la preuve. L'absence de bonne foi constitue au fond la preuve d'une tentative visant à contourner le mécanisme prévu par la loi et les mesures destinées à protéger la vie privée. Recevoir la preuve dans de pareilles circonstances pourrait être susceptible de déconsidérer l'administration de la justice.

RECOMMANDATIONS

54. Lorsque le ministère public entend présenter, à l'enquête préliminaire ou au procès portant sur des infractions non désignées dans une autorisation, des preuves primaires obtenues grâce à celle-ci, le juge qui préside l'instance devrait avoir l'obligation de tenir un voir-dire afin de déterminer si l'interception des preuves touchant ces infractions a été effectuée de bonne foi.

206. Voir la décision du juge Anderson dans *R.* v. *Chambers*, *supra*, note 107.

207. *R.* c. *Commisso*, [1983] 2 R.C.S. 121, 7 C.C.C. (3d) 1.

208. *Id.*, p. 142 (R.C.S.), p. 11 (C.C.C.).

55. Pour l'application de la recommandation 54, l'expression «bonne foi» a la signification suivante :

a) au moment de la demande d'autorisation ou de renouvellement, il était raisonnablement impossible de prévoir l'obtention de preuves relatives à des infractions non désignées dans la demande;

b) si l'on prévoyait obtenir des éléments de preuve relatifs à d'autres infractions, celles-ci n'ont pas été désignées dans la demande parce qu'il ne s'agissait pas d'infractions susceptibles de donner lieu à une autorisation *et* qu'elles ne formaient pas l'objet principal de l'enquête, mais n'étaient *qu'indirectement reliées* à l'enquête sur les infractions désignées dans l'autorisation;

c) au moment de la demande ou du renouvellement, on a déclaré au juge à quelles autorités l'on entendait remettre les renseignements obtenus grâce à l'interception;

d) lorsque les éléments de preuve concernent une infraction à l'égard de laquelle il était possible d'obtenir une autorisation, et si l'on croyait possible d'obtenir des preuves de cette infraction, cette croyance a été divulguée dans les documents présentés à l'appui de la demande *et* l'infraction n'a pas été désignée dans l'autorisation pour les seules raisons suivantes :

(i) les soupçons n'étaient pas suffisants pour satisfaire au critère prévu par la loi;

(ii) l'enquête sur l'infraction en question ne constituait pas le but principal de l'enquête, mais n'en était *qu'un but secondaire*.

56. S'il n'est pas convaincu que l'interception relative aux autres infractions a été effectuée de bonne foi, le juge devrait être tenu d'écarter les preuves primaires et être autorisé à écarter les preuves dont le caractère dérivé est démontré, dès lors qu'il est persuadé que leur réception en preuve est susceptible de déconsidérer l'administration de la justice.

B. Le recours en cas de dérogation au régime législatif

(1) Introduction

Dans le cadre de ses recherches sur les pouvoirs de la police, la Commission de réforme du droit cherche à déterminer les sanctions appropriées en cas de dérogation par les agents de l'État aux règles prévues par la loi. L'adoption du paragraphe 24(2) de la *Charte canadienne des droits et libertés* a mis l'accent sur l'exclusion de la preuve comme mécanisme approprié d'application de la loi. La Commission a néanmoins jugé bon d'étudier des variantes de la règle établie au paragraphe 24(2) comme critère de

l'exclusion de la preuve; des règles ont été proposées dans les rapports intitulés *L'interrogatoire des suspects*[209] et *Les méthodes d'investigation scientifiques*[210]. Il ressort de la discussion qui va suivre que le critère de l'exclusion de la preuve en matière de surveillance électronique est différent, puisqu'il est à la fois plus strict à certains égards, et plus libéral à d'autres égards, en particulier en ce qui a trait au défaut dans la procédure de la demande. Il se peut qu'à une date ultérieure, on tente d'établir une règle uniforme, mais à l'heure actuelle, nous jugeons que la règle d'exclusion spécifique en matière de surveillance électronique peut se justifier.

Il faut tout d'abord reconnaître que, contrairement à d'autres aspects de l'étude des pouvoirs de la police, il existait déjà au moment où nous avons entrepris l'analyse de la question de la surveillance électronique, une règle d'exclusion stricte à l'égard de la preuve primaire (la communication elle-même), et une règle d'exclusion moins stricte à l'égard de la preuve qui en découle, semblable à la règle prévue au paragraphe 24(2) de la Charte. Il faut également se rappeler qu'il s'agit peut-être du dispositif d'enquête le plus attentatoire que le Parlement ait jamais autorisé. Lorsque ce projet a été adopté, l'on a reconnu que la Partie IV.1 donnait à la police des pouvoirs d'enquête étendus, tout en imposant aux organismes chargés de l'application de la loi l'obligation de respecter intégralement le mécanisme prévu. En conséquence, la police et le ministère public ont formé des spécialistes pour préparer les demandes et mettre les autorisations en application, et l'on peut raisonnablement s'attendre à un niveau élevé de respect de la loi. La critique la plus fréquente de la règle d'exclusion est qu'elle nuit à «l'agent dans le feu de l'action» qui doit agir rapidement dans des situations d'urgence et qui n'a pas toujours la formation juridique nécessaire; cette critique ne s'applique tout simplement pas dans ce contexte.

Enfin, le principe même du mécanisme prévoyant la légalisation des tables d'écoute exige que l'on fasse appel au processus judiciaire et permet au tribunal de tenir un rôle de surveillance important grâce au seul moyen efficace disponible, à savoir le contrôle du processus judiciaire et de la recevabilité de la preuve. Dans ce contexte, même la règle de l'exclusion absolue n'est pas très différente du critère modifié — «leur utilisation est susceptible de déconsidérer l'administration de la justice» — que la Commission propose dans d'autres rapports, puisqu'il est manifeste que le défaut de respecter l'ordonnance d'un tribunal dénote un certain manque de respect à l'égard de l'administration de la justice.

(2) La question de l'exclusion en général

La présente partie traite de la recevabilité de la preuve. Certaines règles spéciales ont déjà été abordées en raison des principes importants et spécifiques en jeu dans ces

209. Commission de réforme du droit du Canada, *L'interrogatoire des suspects* [Rapport 23], Ottawa, Ministère des Approvisionnements et Services, 1984.

210. Commission de réforme du droit du Canada, *Les méthodes d'investigation scientifiques : l'alcool, la drogue et la conduite des véhicules* [Rapport 21], Ottawa, Ministère des Approvisionnements et Services, 1983.

domaines, notamment en matière d'interceptions à l'étranger (recommandations 11 à 13) et d'interceptions relatives à d'autres infractions (recommandations 55 et 56).

Dans la présente partie, nous examinons plus précisément le problème de l'exclusion de la preuve comme premier moyen d'application du mécanisme prévu par la loi. Même si nous traitons brièvement de la règle de l'exclusion en général, telle qu'elle est formulée à l'article 178.16 du *Code criminel*, le vrai problème se situe au niveau de l'effet d'une procédure de révision. Pour situer le débat, nous avons établi deux versions de la définition d'un vice de fond dans la demande. Il faut se rappeler que nous recommandons l'exclusion de la preuve comme sanction d'un vice de fond dans la demande. Les deux formulations expriment les paramètres de la règle de l'exclusion dans le contexte de la révision. Ces deux formulations, que nous pouvons décrire comme «A» : la règle de l'exclusion absolue, et «B» : la règle de l'exception fondée sur la bonne foi, sont les suivantes :

Formule «A» : l'exclusion absolue

Un vice de fond dans la demande signifie :

a) qu'aucune des conditions préalables énoncées à l'alinéa 178.13(1)*b*) n'existait; ou

b) que l'on n'avait aucun motif raisonnable et probable de croire qu'une personne désignée dans l'autorisation était en train de commettre l'infraction visée; ou

c) qu'il existe d'autres raisons permettant raisonnablement de conclure que si la véritable situation avait été connue, l'autorisation n'aurait pas été accordée, ou qu'elle l'aurait été sous une forme substantiellement différente.

Formule «B» : l'exception fondée sur la bonne foi

La demande devrait être être considérée comme entachée d'un vice de fond si, en raison d'énoncés dans la demande ou l'affidavit qui, à la connaissance des enquêteurs, étaient faux, d'énoncés qui ont été faits sans que l'on se soucie de leur véracité ou de leur fausseté, ou d'omissions délibérées ou faites par insouciance, il est établi

a) qu'aucune des conditions préalables énoncées à l'alinéa 178.13(1)*b*) n'existait; ou

b) que l'on n'avait aucun motif raisonnable et probable de croire qu'une personne désignée dans l'autorisation était en train de commettre l'infraction visée; ou

c) qu'il existe d'autres raisons permettant raisonnablement de conclure que si la véritable situation avait été connue, l'autorisation n'aurait pas été accordée, ou qu'elle l'aurait été sous une forme substantiellement différente.

Pour préciser davantage les points en question, nous étudions la décision récente de la Cour suprême des États-Unis dans l'affaire *United States* v. *Leon*[211], où la Cour a reconnu pour la première fois une exception, fondée sur la bonne foi, à la règle d'exclusion découlant du quatrième amendement, dans des circonstances qui sont d'une grande pertinence pour la présente étude, à savoir l'exécution de bonne foi d'un mandat judiciaire. Nous étudierons ensuite la justification de la règle d'exclusion et donnerons nos recommandations en ce domaine. Il faut dire qu'il s'agit de questions de principe difficiles, et que nous sommes en faveur d'un recours qui concilie les intérêts contraires. La décision dans l'affaire *Leon* représente un effort important de conciliation dans le contexte américain. Le paragraphe 24(2) de la Charte constitue également une recherche d'équilibre dans le contexte d'une violation des garanties constitutionnelles. Nous ne recommandons en fin de compte que très peu de modifications à la règle d'exclusion qui est actuellement prévue à la Partie IV.1; la plupart de nos recommandations visent à clarifier la procédure et les règles.

À l'heure actuelle, en vertu de la Partie IV.1 du *Code criminel*, la règle d'exclusion s'applique à divers égards :

a) lorsque le préavis prévu au paragraphe 178.16(4) n'a pas été donné de façon adéquate;

b) lorsqu'il n'y a ni autorisation ni consentement, c'est-à-dire lorsqu'il s'agit d'une interception illégale;

c) lorsqu'il y a une autorisation, mais que l'interception n'est pas effectuée en conformité avec celle-ci, par exemple à l'égard des communications d'une personne dont le nom ne figure pas dans l'autorisation;

d) lorsqu'une autorisation est révisée et révoquée.

Tous ces éléments s'appliquent uniquement à la preuve primaire, c'est-à-dire à la communication elle-même; un critère différent s'applique à la preuve dérivée.

Nos recommandations modifieraient la situation visée à l'alinéa a) (préavis), mais nous ne proposons aucune modification aux situations visées aux alinéas b) (interception illégale sans consentement) et c) (non-respect de l'autorisation). Puisque nous proposons une modification des sanctions à l'égard du préavis, nous en discuterons plus loin. Cependant, nous devons d'abord étudier brièvement la question du respect de l'autorisation. Avant l'arrêt de la Cour suprême du Canada dans l'affaire *Lyons* c. *La Reine*[212], on n'était pas certain de la portée exacte de la condition de recevabilité prévue à l'alinéa 178.16(1)*a*), qui exige que l'interception soit «faite légalement». Le jugement de la majorité dans l'affaire *Lyons* règle le problème d'une façon entièrement satisfaisante, qui respecte à la fois les principes de l'inviolabilité de la vie privée et les exigences de l'application efficace de la loi.

211. *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

212. *Supra*, note 123.

Dans l'arrêt *Lyons*, le juge Estey déclare au nom de la majorité que le processus d'interception est une entreprise unique réalisée en vertu d'une autorisation et qu'il ne peut se diviser en étapes comportant des conséquences juridiques et en étapes n'en comportant pas. Ainsi, un acte illicite accompli dans l'installation du dispositif pourrait entacher la légalité de l'interception. La Cour d'appel de l'Ontario a tiré une conclusion semblable dans deux affaires récentes : *R.* v. *Papalia*[213] et *R.* v. *McCafferty*[214]. On a également conclu cependant que l'expression «faite légalement» de l'alinéa 178.16(1)*a*) ne signifie pas en conformité avec toutes les lois, mais plutôt avec la Partie IV.1. Par conséquent, l'entrée clandestine en vue d'installer le dispositif après l'obtention de l'autorisation serait légale. Cependant, si elle a eu lieu avant que l'autorisation soit accordée, peut-être sous le couvert d'un mandat de perquisition (comme dans l'affaire *McCafferty*), alors l'interception n'aurait pas été exécutée aux termes d'une autorisation, et par conséquent elle n'aurait pas été faite légalement, même si aucun enregistrement n'avait été effectué avant l'obtention de l'autorisation.

C. Le préavis en vertu du paragraphe 178.16(4)

Les dispositions actuelles de la Partie IV.1, en particulier le paragraphe 178.16(4), exigent du ministère public qu'il donne à l'accusé un préavis raisonnable de son intention de produire la communication privée. Le préavis doit être donné dans un délai raisonnable et contenir une indication de l'heure, de la date et du lieu de la communication privée. De même, une transcription de la communication doit être fournie si l'enregistrement magnétique est joué; autrement, une déclaration donnant tous les détails de la communication privée est exigée. À défaut de ces documents, la preuve est irrecevable. Dans sa formulation, la disposition prévoyant le préavis s'applique à une communication privée interceptée légalement, ce qui semble renvoyer uniquement à la condition énoncée à l'alinéa 178.16(1)*a*), c'est-à-dire la preuve d'une communication privée qui est recevable lorsque l'interception a été faite légalement, et non à la condition prévue à l'alinéa 178.16(1)*b*) qui permet la réception d'une preuve, peu importe les moyens utilisés pour l'obtenir, pourvu qu'il y ait eu consentement d'une des parties à la communication, et pas nécessairement celui de l'accusé. Les exigences en matière de préavis énoncées au paragraphe 178.16(4) servent beaucoup plus à mettre l'autre partie au courant qu'à protéger la vie privée. À notre avis, la fonction de divulgation s'applique peu importe que la preuve ait été produite en vertu de l'alinéa 178.16(1)*a*) ou *b*). La jurisprudence veut cependant qu'aucun préavis ne soit exigé lorsque la preuve est produite avec le consentement d'une des parties[215]. Selon nous, la distinction ne repose sur aucun argument valable. D'autre part, la loi prévoit que la sanction d'un défaut de préavis est l'exclusion de la preuve. Cela semble être une sanction draconienne dans des dispositions conçues essentiellement pour remplir une fonction de divulgation.

213. *R.* v. *Papalia*, (1984) 13 C.C.C. (3d) 449 (C.A. Ont.).

214. *Supra*, note 147.

215. Voir *R.* v. *Banas and Haverkamp*, (1982) 65 C.C.C. (2d) 224 (C.A. Ont.) et *R.* v. *McDonald and Tondu*, (1981) 60 C.C.C. (2d) 336 (C.A Alb.).

À notre avis, l'exclusion de la preuve devrait être réservée aux manquements graves aux dispositions, et le mécanisme de contrôle primaire dans ce domaine devrait viser le respect du processus. Si la dérogation aux dispositions en matière de préavis entraîne des délais déraisonnables, il existe des recours en vertu de la *Charte canadienne des droits et libertés*[216].

Bien sûr, comme nous l'avons proposé plus haut, on devrait donner plus d'extension aux exigences en matière de préavis afin d'exiger du ministère public qu'il produise une copie de l'autorisation ou du renouvellement, de même que des documents visés à l'article 178.14 qui ne sont pas touchés par une ordonnance de non-divulgation d'un tribunal. Il faut cependant appliquer le même raisonnement, puisque le défaut de respecter les conditions n'entraînerait pas l'exclusion de la preuve, mais seulement des sanctions destinées à assurer le respect de la loi.

Par le passé, la question s'est posée de savoir si l'article 178.16 s'applique à des audiences relatives à la mise en liberté sous caution. Dans une décision récente, *R.* v. *Kevork*[217], le juge Ewaschuk est d'avis que la formulation de l'alinéa 457.3(1)*e*), qui permet au juge d'écarter les conditions préalables strictes en matière de recevabilité de la preuve, signifie que l'article 178.16 ne s'applique pas aux audiences en matière de mise en liberté provisoire. Qu'il s'agisse ou non de l'interprétation correcte des articles 457.3 et 178.16, nous sommes d'avis que la preuve d'une communication privée interceptée ou celle qui en découle devrait être admissible à de telles audiences, sans que l'on doive recourir à une enquête stricte sur la légalité de l'interception, pourvu que celle-ci ait apparemment été exécutée en vertu d'une autorisation ou avec le consentement d'une partie. À cet égard, nous soulignons la modification apportée au paragraphe 457.3(1) du *Code* aux termes du paragraphe 85(1) du projet de loi C-18 (adopté par la Chambre des communes le 24 avril 1985) qui ajoutera l'alinéa *d*.1) suivant :

> le juge de paix peut admettre en preuve par écrit, de vive voix, ou sous forme d'enregistrement, une communication privée qui a été interceptée au sens de la partie IV.1; le paragraphe 178.16(4) ne s'applique pas au présent article; ...

Cependant, la formulation de ce nouveau texte pourrait être améliorée en établissant clairement qu'il doit s'appliquer à la fois à la communication elle-même et à la preuve qui en dérive.

D. Le vice de fond dans la demande

Le vrai problème qui se pose en matière de recevabilité de la preuve concerne la vérification de la demande d'autorisation.

---

216. En particulier le droit d'être jugé dans un délai raisonnable énoncé à l'alinéa 11*b*).

217. *R.* v. *Kevork*, (1984) 12 C.C.C. (3d) 339 (Haute cour Ont.).

En bref, le dilemme est le suivant : comment peut-on justifier l'exclusion de la preuve lorsque celle-ci a été recueillie par la police dans l'exécution d'un mandat judiciaire? Si le mécanisme prévu par la loi vise à exiger le contrôle judiciaire avant l'interception, quelles sont les vraies raisons qui justifieraient d'exclure une preuve lorsqu'un juge a étudié le fond de la demande et, dans l'exercice d'une fonction judiciaire, a autorisé l'intrusion? Il existe, bien sûr, un cas où la protection accordée par le mécanisme prévu par la loi est annulée par la conduite de la police. Il s'agit de la situation décrite par la formule «B». Le juge appelé à donner une autorisation n'est pas vraiment en position d'évaluer adéquatement le bien-fondé de la demande et protéger ainsi le public d'une intrusion non nécessaire, si l'on ne lui a pas dit toute la vérité, intentionnellement ou par insouciance. En pareil cas, comme dans l'affaire *Gill*[218], la nécessité de l'exclusion de la preuve pour décourager pareille conduite ressort clairement.

Le cas est moins clair lorsque les autorités qui ont présenté une demande adéquate, se sont fiées à la décision du juge qui a accepté la demande, et ont agi de bonne foi sur la base de l'autorisation, voient finalement la preuve exclue parce qu'un autre juge détermine, par exemple, que les documents n'ont pas divulgué des motifs raisonnables et probables pouvant justifier une interception.

La distinction entre les deux situations a fait l'objet d'une étude par la Cour suprême des États-Unis dans l'affaire *United States* v. *Leon*[219]. Le juge White, qui a rendu le jugement au nom de la majorité, a établi une exception, fondée sur la bonne foi, à la règle de l'exclusion absolue de la preuve obtenue en contravention des droits protégés par le quatrième amendement. La majorité des juges, qui ont reconnu l'inexistence d'une cause plausible justifiant la délivrance d'un mandat de perquisition, ont néanmoins conclu que la preuve reçue en vertu de ce mandat était admissible. Le juge White est d'avis que la raison d'être de la règle de l'exclusion est de dissuader la police d'agir illégalement, et que cette raison n'était pas suffisamment forte dans le cas de l'exécution de bonne foi d'un mandat.

Le juge White reprend longuement la question du fondement de la règle de l'exclusion, et en particulier la notion de dissuasion, et conclut que [TRADUCTION] «si par conséquent, l'exclusion de la preuve obtenue en vertu d'un mandat jugé par la suite invalide doit avoir un effet de dissuasion, il faut qu'elle modifie le comportement de chacun des agents de la paix ou les politiques de leurs divisions»; il conclut en outre que [TRADUCTION] «la suppression de la preuve obtenue en vertu d'un mandat ne devrait être ordonnée qu'à la suite d'un examen de l'espèce, et seulement dans les cas où l'exclusion favoriserait les fins de la règle de l'exclusion[220]».

La protection accordée aux droits relatifs à la vie privée par la Partie IV.1 du *Code criminel* s'apparente à celle prévue par le quatrième amendement (et son équivalent canadien, l'article 8 de la *Charte canadienne des droits et libertés*). La Cour suprême

218. *Supra*, note 116.

219. *Supra*, note 211.

220. *Id.*, p. 3419.

des États-Unis a déterminé que l'exclusion de la preuve ne constitue pas le moyen approprié pour protéger ces droits constitutionnels en certaines circonstances lorsqu'on tient compte des coûts (il s'agit essentiellement de l'acquittement du coupable) et des bénéfices (effet dissuasif à l'égard de toute violation future du quatrième amendement). Quels sont donc les arguments contre l'exception fondée sur la bonne foi?

Des motifs de dissidence très vigoureux ont été rédigés par le juge Brennan (auxquels a souscrit le juge Marshall). Le juge avait entrevu cette tournure à cause de la façon dont la Cour suprême avait tranché les questions relatives au quatrième amendement au cours des dix dernières années. De plus, les exceptions fondées sur la bonne foi ont suscité un débat doctrinal qui dure depuis au moins dix ans et qui devait être relancé récemment par la décision *United States* v. *Williams*[221], où la Cour d'appel des États-Unis du cinquième circuit siégeant en banc a établi une large exception fondée sur la bonne foi.

Dans ses motifs de dissidence, le juge Brennan adopte une vision beaucoup plus large du fondement de la règle de l'exclusion. Il ne considère pas qu'elle repose principalement sur la théorie de la dissuasion[222].

Le juge Brennan rejette la théorie étroite de la dissuasion, la jugeant invérifiable. Il cite les paroles du juge Stewart dans l'affaire *Faretta* v. *California*[223] : [TRADUCTION] «les libertés individuelles ne sont pas fondées sur la loi des moyennes[224]». D'autre part, il minimise les coûts de la règle de l'exclusion, en soulignant que la preuve non assujettie à la règle de l'exclusion en raison de la violation du quatrième amendement serait vraisemblablement suffisante pour entraîner une condamnation[225]. Le juge Brennan reprend cependant une théorie institutionnelle de la dissuasion, suivant laquelle le fait de démontrer [TRADUCTION] «que notre société attache de sérieuses conséquences à la violation des droits constitutionnels est perçu comme un encouragement pour ceux qui formulent les politiques d'application de la loi, et les agents qui les mettent en œuvre, à incorporer les idéaux du quatrième amendement dans leur système de valeurs[226]».

En ce qui a trait plus précisément à la question du mandat, le juge Brennan estime que la doctrine de la bonne foi est dangereuse puisqu'elle peut très bien inciter graduellement les agents de la paix et les magistrats à négliger la préparation et l'étude attentive des demandes.

Dans ses motifs de dissidence, le juge Stevens concentre son attention sur les fins du quatrième amendement, et sur un aspect du débat qui semble oublié, soit le fait que le quatrième amendement trouve son origine historique dans l'abus de la procédure

221. *United States* v. *Williams*, 622 F.2d 830 (1980), demande rejetée 449 U.S. 1127 (1981).

222. *United States* v. *Leon*, *supra*, note 211, p. 3436-3437.

223. *Faretta* v. *California*, 422 U.S. 806 (1975).

224. *Id.*, p. 834.

225. *United States* v. *Leon*, *supra*, note 211, p. 3439.

226. *Id.*, p. 3443.

du mandat et dans le désir des rédacteurs de la Constitution de protéger le citoyen des mandats et des ordonnances de main-forte généraux. Historiquement, le [TRADUCTION] «cas type de la perquisition abusive était l'exécution d'un mandat non fondé sur une cause probable[227]». Il voit dans la règle d'exclusion un mécanisme destiné à prévenir la violation du quatrième amendement, et dans l'exception fondée sur la bonne foi une doctrine en voie de causer [TRADUCTION] «de graves dommages à cette fonction de dissuasion[228]». Il exprime aussi son inquiétude face à la tendance des tribunaux à négliger leur responsabilité à l'égard des violations de nature constitutionnelle.

Nous voyons ainsi les deux côtés d'un débat présenté dans une affaire constitutionnelle qui fera peut-être autorité aux États-Unis, où une règle d'exclusion absolue est appliquée depuis près de vingt-cinq ans dans les poursuites intentées par les États[229], et depuis près de soixante-dix ans dans les poursuites intentées par le gouvernement fédéral[230]. L'étude de cette expérience pourrait être de quelque utilité dans notre recherche de la règle appropriée pour régir la surveillance électronique au Canada. Même s'il faut souligner que le débat aux États-Unis se situe dans un contexte supposant l'application d'une garantie constitutionnelle, cela ne diminue en rien sa pertinence. Le respect de la vie privée, peu importe qu'il soit consacré dans une constitution, est de plus en plus perçu comme un droit important, voire fondamental, de la société moderne. Le droit à l'intimité de la vie privée et la modération dans les atteintes qui peuvent lui être portées sous-tendent la plupart des travaux de la section de recherche sur les pouvoirs de la police, tout particulièrement lorsque l'on considère les possibilités d'utilisation d'un mécanisme aussi attentatoire que celui de la surveillance électronique.

Quel est donc le fondement de la règle de l'exclusion de la preuve?

a) *Elle procéderait de la Constitution*. Cette théorie s'est élaborée aux Étas-Unis sur la base suivante : l'utilisation de documents saisis en violation du quatrième amendement se trouverait à transgresser la garantie du cinquième amendement contre l'auto-accusation[231]. La théorie n'est plus acceptée de façon générale aujourd'hui[232]. Il s'agit cependant d'une théorie qui a une certaine importance dans le contexte canadien, puisque le paragraphe 24(2) de la *Charte canadienne des droits et libertés* contient une règle d'exclusion explicite, quoique limitée. Selon cette théorie, l'exclusion de la preuve obtenue par l'écoute électronique serait justifiée *si* les droits constitutionnels de l'accusé étaient violés *et* si les critères du paragraphe 24(2) s'appliquaient. La bonne foi de la part des autorités est certainement un important élément de l'équation «eu égard aux circonstances[233]».

227. *Id.*, p. 3453.

228. *Id.*, p. 3454.

229. Depuis *Mapp* v. *Ohio*, 367 U.S. 643 (1961).

230. Depuis *Weeks* v. *United States*, 232 U.S. 383 (1914).

231. *Supra*, note 229.

232. Potter Stewart, «The Road to *Mapp* v. *Ohio* and Beyond : The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases», (1983) 83 *Colum. L. Rev.* 1365, p. 1381.

233. Voir *R.* v. *Simmons*, *supra*, note 86 et *R.* v. *Rao*, *supra*, note 46.

Toute règle d'exclusion plus large ou différente doit par conséquent reposer sur d'autres bases. Il est nécessaire d'étudier celles-ci plus en profondeur pour deux motifs : en premier lieu, on ne sait pas très bien quelles sont les violations du régime législatif de l'écoute électronique qui entraînent un effet constitutionnel, et l'on sait encore moins quand la réception d'une preuve ainsi obtenue serait susceptible de déconsidérer l'administration de la justice. En deuxième lieu, on peut s'attendre à ce que les violations de la constitution se règlent d'elles-mêmes. Aucun mécanisme prévu par une loi n'est requis. Même si, en matière de violation de la constitution, le Parlement a adopté un critère beaucoup moins rigide que celui de l'exclusion absolue, cela n'empêche pas le législateur d'adopter, lorsque cela est justifié, une règle semblable ou différente.

b) *L'exclusion servirait à préserver l'intégrité de l'État et des tribunaux*. Selon cette théorie, l'exclusion est nécessaire afin d'empêcher que le gouvernement n'obtienne l'aide de l'ordre judiciaire pour donner effet à une violation du quatrième amendement, et empêcher les tribunaux de commettre eux-mêmes une deuxième violation du même amendement. Encore une fois, même s'il s'agit d'une théorie qui n'est pas très bien reçue aux États-Unis[234], elle a une certaine pertinence dans le débat canadien; en fait, elle apporte une réponse à certains des problèmes en matière d'exclusion. Dans le contexte de l'écoute électronique, la question peut être posée de la façon suivante : s'il acceptait la preuve, le tribunal pourrait-il être partie à la perpétration d'une infraction criminelle? Il s'agit là de l'argument principal sous-jacent à l'exclusion de la preuve dans l'affaire *R.* v. *Stewart*[235], même si, à première vue, la règle n'exigeait pas l'exclusion. Même si la règle normale au Canada veut que la preuve obtenue illégalement soit admissible, cette règle ne s'applique pas aux situations où [TRADUCTION] «l'utilisation ou la divulgation de la preuve au cours du procès est illégale[236]», puisqu'en pareil cas, l'intention du Parlement est certainement d'exclure la preuve.

Il y a manifestement une certaine facticité à ce fondement, dans le contexte de la réforme du droit, puisque les réformateurs auraient la liberté de modifier la règle de l'exclusion en redéfinissant les infractions. En tenant compte de ce fait, cependant, quels aspects du régime ce fondement de la règle d'exclusion embrasse-t-il? Aux fins de notre étude, il faut procéder à une analyse de la disposition prévoyant l'exonération de responsabilité à l'égard de l'infraction de divulgation créée par les paragraphes 178.2(1) et (2) :

(2) Le paragraphe (1) ne s'applique pas à une personne qui divulgue soit tout ou partie d'une communication privée ou la substance, le sens ou l'objet de tout ou partie de celle-ci, soit l'existence d'une communication privée

234. Potter Stewart, *loc. cit. supra*, note 232, p. 1382-1383.

235. *R.* v. *Stewart*, (1981) 60 C.C.C. (2d) 407 (C.A. Ont.).

236. *Id.*, p. 437.

> *a*) au cours ou aux fins d'une déposition lors de poursuites civiles ou pénales ou de toutes autres procédures dans lesquelles elle peut être requise de déposer sous serment lorsque la communication privée est admissible en preuve en vertu de l'article 178.16 ou le serait en vertu de cet article s'il s'appliquait aux poursuites ou procédures;
>
> *b*) au cours ou aux fins d'une enquête en matière pénale, si la communication privée a été interceptée légalement; ...

Cette disposition renvoie à l'alinéa 178.16(1)*a*) et à l'obligation de procéder à une interception légalement, et partant, à l'article 178.11 qui donne les paramètres d'une interception légale. Aux fins de la présente discussion, nous devons étudier deux situations : les interceptions effectuées avec le consentement des intéressés (alinéa 178.11(2)*a*)) et les interceptions autorisées (alinéa 178.11(2)*b*)). La dernière disposition est la plus importante et elle prévoit que le texte d'incrimination ne s'applique pas

> ... à une personne qui intercepte une communication privée en conformité d'une autorisation ni à une personne qui, de bonne foi, aide de quelque façon une autre personne qu'elle croit, en se fondant sur des motifs raisonnables et probables, agir en conformité d'une telle autorisation; ...

Par conséquent, l'exclusion de la preuve vise à éviter la perpétration d'une infraction lorsque l'interception n'a pas eu lieu en conformité d'une autorisation. C'est la position actuelle au Canada[237], et nous ne proposons pas d'y apporter des modifications. Comme nous l'avons indiqué plus haut, cette règle devrait être maintenue. Il faut remarquer qu'une interception de «bonne foi» faite en conformité d'une autorisation n'exonère pas toutes les parties qui ont procédé à l'interception, mais seulement les personnes, comme les employés de téléphone, qui ont aidé les responsables à procéder à l'interception. On ne peut donc faire valoir une exception fondée sur la bonne foi au regard de la condition de recevabilité qu'énoncent les termes «en conformité d'une autorisation».

D'autre part, cette analyse ne résout pas vraiment le problème de la révision de l'autorisation. Il serait bien sûr possible de créer une fiction voulant que s'il existe un vice de fond dans la demande, l'autorisation est alors cassée[238], de sorte qu'en droit, les agents n'agissaient pas conformément aux dispositions de l'autorisation et, partant, agissaient illégalement en vertu du paragraphe 178.11(1). Une telle condamnation rétroactive irait à l'encontre des notions habituelles de justice, même en ne tenant pas compte des questions subtiles du *mens rea* ni de l'application de l'alinéa 11*g*) de la *Charte canadienne des droits et libertés*. Il serait plus utile d'aborder le problème de la révision directement en reconnaissant le fait que les autorités ont procédé à l'interception conformément à une autorisation qui était alors valide, et de se demander si, nonobstant ce fait et le fait qu'elles n'ont commis aucune infraction en exécutant l'autorisation et qu'elles n'en commettraient aucune en produisant la preuve ainsi obtenue en cour, il existe un autre fondement pour exclure la preuve lorsque l'autorisation est entachée d'un vice de fond.

---

237. Voir *R.* v. *Welsh and Innuzzi (No. 6)*, *supra*, note 31 et *R.* v. *Niles*, *supra*, note 163.

238. *Wilson* v. *The Queen*, *supra*, note 167.

En vertu de la théorie de l'exclusion comme sanction nécessaire à l'application du régime, l'exclusion de la preuve est nécessaire au regard du quatrième amendement afin d'assurer que le gouvernement ne transgresse pas les dispositions de cet amendement. Elle n'est justifiée que s'il n'existe aucun autre moyen adéquat d'application[239]. Là se trouve le centre du débat sur l'effet de dissuasion, ainsi que la justification de l'exception fondée sur la bonne foi. C'est dans ce contexte que les motifs, s'il en est, de l'exclusion de la preuve dans tous les cas s'imposent lorsque la procédure de demande d'autorisation comporte des vices (ou a été l'objet de violations). Il faut tenir compte des coûts et des avantages d'une règle d'exclusion de la preuve, et de ceux des autres recours disponibles.

Il faudrait souligner que tout comme dans le débat sur la règle de l'exclusion en vertu du quatrième amendement, une chose est sûre : il vaut mieux que les autorités respectent le mécanisme prévu par la loi (comme c'est une bonne chose que les autorités aux États-Unis respectent le quatrième amendement). Si l'on cherche à établir des recours de toute nature en cas de violation des dispositions de la loi, c'est que l'on veut s'assurer que le régime en vigueur continue d'offrir une protection efficace contre les violations des règles et contre toute atteinte au droit à l'intimité de la vie privée. À cet égard, il convient de poser deux questions :

1. Quelles sont les fins visées par toute forme de recours?

   a) La dissuasion spécifique : dissuader l'agent de commettre de nouveau la même violation du mécanisme prévu par la loi.

   b) La dissuasion générale : dissuader les autres agents de commettre la même violation du mécanisme prévu par la loi.

   c) La dissuasion systémique : encourager les autorités à mettre en place des mesures afin d'empêcher des violations subséquentes.

2. Quels sont les recours autres que l'exclusion de la preuve?

(1) Le recours en droit délictuel

Comme solution de rechange à l'exclusion de la preuve pour assurer un plus grand respect du mécanisme, on pourrait établir dans la loi un recours en droit délictuel qui habiliterait la victime d'une interception autorisée de façon inadéquate à poursuivre les autorités. De l'avis de pratiquement tous les auteurs américains, cette méthode serait inefficace[240].

239. Potter Stewart, *loc. cit. supra*, note 232, p. 1384.

240. William J. Mertens et Silas Wasserstrom, «The Good Faith Exception to the Exclusionary Rule: Deregulating the Police and Derailing the Law», (1981) 70 *Geo. L.J.* 365, p. 406-410; Stewart, *loc. cit. supra*, note 232, p. 1387-1388; William A. Schroeder, «Deterring Fourth Amendment Violations: Alternatives to the Exclusionary Rule», (1981) 69 *Geo. L.J.* 1361, p. 1386-1396.

Nous sommes également d'avis, pour bon nombre de motifs semblables, qu'un tel recours en droit délictuel inscrit dans la loi serait un moyen inefficace d'assurer le respect du mécanisme prévu par la Partie IV.1. De plus, jusqu'à maintenant, les recours au civil n'ont jamais été le meilleur moyen pour réparer des violations ou assurer l'application de la loi. La Partie I.1 de la *Loi sur la responsabilité de la Couronne*[241] et l'article 178.21 du *Code criminel* prévoient le paiement de dommages-intérêts en cas d'interception ou de divulgation illégales par des agents de la Couronne ou par des particuliers. À notre connaissance, aucune poursuite (couronnée de succès ou non) n'a jamais été intentée contre un agent à l'égard d'une activité liée à la surveillance électronique, même s'il est possible de prétendre que, lorsque la preuve est exclue en vertu de l'alinéa 178.16(1)*a*), une poursuite en responsabilité civile délictuelle peut être intentée.

(2) La responsabilité pénale

Une autre solution consisterait à étendre la responsabilité pénale en créant des infractions destinées à assurer le respect de la procédure de demande. Encore une fois, l'expérience démontre qu'il ne s'agit pas d'un recours permettant d'assurer efficacement le respect du mécanisme[242].

C'est un fait connu, il est difficile d'obtenir la condamnation d'agents de police même pour des accusations d'inconduite scandaleuse. Nous ne cherchons pas à juger de quelque façon de la validité de ces prétentions, mais les obstacles institutionnels, notamment la preuve du *mens rea*, la preuve à établir au-delà d'un doute raisonnable et la collaboration de confrères policiers pour fournir la preuve, diminuent la force de la menace de poursuites pénales comme moyen efficace d'appliquer la loi. Encore une fois, l'expérience découlant de l'application de la Partie IV.1 confirme cette impression. Le paragraphe 178.22(3) exige que le rapport annuel du procureur général ou du solliciteur général contienne «le nombre de poursuites intentées contre des fonctionnaires ou préposés de Sa Majesté du chef du Canada ou des membres des Forces canadiennes pour des infractions prévues aux articles 178.11 ou 178.2». Nous n'avons pu trouver aucun rapport faisant état de telles poursuites. De plus, nous ne sommes au courant d'aucune poursuite contre un membre d'une force de police municipale ou provinciale[243].

(3) Le contrôle extrajudiciaire

Sous cette rubrique peuvent figurer les commissions de révision indépendantes et les procédures de discipline interne. Dans la mesure où le mécanisme de ces recours

241. *Loi sur la responsabilité de la Couronne*, S.R.C. 1970, chap. C-38, modifiée par S.C. 1973-1974, chap. 50, art. 4.

242. Voir Schroeder, *loc. cit. supra*, note 240, p. 1396-1398 et Stewart, *loc. cit. supra*, note 232, p. 1386-1387.

243. Bien que nous ayons recommandé la création d'une infraction pour le fait d'entrer subrepticement et sans autorisation dans des lieux, nous admettons qu'il s'agit dans une certaine mesure d'une démarche symbolique qui reflète néanmoins la gravité de cette intrusion à nos yeux.

serait déclenché par des poursuites intentées par les citoyens, il souffrirait des mêmes défauts que les recours étudiés plus haut. Même si une commission de révision indépendante pouvait statuer sur les cas renvoyés par des juges du procès, il n'est pas certain que cela donnerait un mécanisme efficace d'application de la loi. Si la façon dont une demande a été faite n'a aucune pertinence légale au procès, alors aucun juge ne serait motivé à relever une violation de la procédure de demande. Au contraire, avec la pression toujours plus grande que subissent les tribunaux en raison des délais et de l'encombrement croissant des rôles, il y a une réticence réelle de la part du juge à se lancer dans des enquêtes qui ne sont pas légalement pertinentes, et il n'y a aucun encouragement de la part de l'accusé ou du ministère public à procéder à l'enquête. Les contrôles internes souffrent des mêmes effets de démobilisation. [TRADUCTION] «Les agents de police ignorent souvent l'inconduite grave d'autres agents, et les tribunaux avisent rarement les administrateurs de la police de l'inconduite de leurs propres agents[244]».

(4) La règle d'exclusion

Il nous reste à étudier la règle d'exclusion. Nous l'analyserons cependant sous un angle très étroit, soit celui de la volonté d'assurer le respect de la procédure de demande par l'exclusion de la preuve dans les cas de non-respect grave. Nous avons déjà établi deux modèles, l'un fondé sur l'exclusion automatique en cas de non-respect, et l'autre fondé sur une exclusion seulement en cas de non-respect de bonne foi. Les coûts susmentionnés de l'exclusion incluent la décision inadéquate qui se traduit normalement par l'acquittement du coupable, l'abandon de poursuites qui sont par ailleurs fondées ou la négociation d'une sentence non appropriée, et le mépris de la loi qui résulte de la perception selon laquelle les coupables sont libérés ou traités de façon inadéquate.

La règle d'exclusion fait l'objet d'une importante critique : à l'instar des autres mesures proposées, elle n'a aucun effet de dissuasion en matière de non-respect.

Abordons en premier lieu la question des coûts. Bien que de nombreuses études aient été entreprises dans le but d'établir ces coûts en termes de poursuites perdues ou abandonnées en raison de la règle d'exclusion fondée sur le quatrième amendement, il est probablement impossible de tirer une conclusion[245]. Les partisans de l'exclusion absolue ont tendance à en minimiser les coûts[246]. Par contre, les partisans de l'abolition de cette règle ont tendance à exagérer ces coûts. On a déjà souligné que, dans les cas graves comme le meurtre, l'effet est exagéré, et que dans la plupart des cas, d'autres

244. Schroeder, *op. cit. supra*, note 240, p. 1401; voir également Stewart, *loc. cit. supra*, note 232, p. 1388.

245. Voir Thomas Y. Davies, «A Hard Look at What We Know (and Still Need to Learn) about the Costs of the Exclusionary Rule: The NIJ Study and Other Studies of ‹Lost› Arrests», (été 1983) 3 *American Bar Foundation Research Journal* 611; Bradley C. Canon, «Ideology and Reality in the Debate over the Exclusionary Rule: A Conservative Argument for Its Retention», (1982) 23 *S. Tex. L.J.* 559; Mertens et Wasserstrom, *loc. cit. supra*, note 240; Schroeder, *loc. cit. supra*, note 240, p. 1382-1385.

246. Stewart, *loc. cit. supra*, note 232, p. 1394.

éléments de preuve sont disponibles[247]. Nous ne cherchons pas à minimiser la gravité de ces coûts, mais plutôt à les présenter d'une façon précise[248]. Quelques poursuites intentées récemment en vertu de la *Charte canadienne des droits et libertés* ont soulevé les mêmes questions[249]. De même, les tentatives visant à déterminer l'effet de dissuasion de la règle sur le comportement de la police ne sont pas concluantes[250]. Il faut par conséquent poursuivre le débat sur la base d'arguments intuitifs[251].

Certains de ces arguments peuvent perdre de leur poids en matière de surveillance électronique en raison de la façon dont les demandes sont préparées. Celles-ci ne sont pas le fait de décisions prises sur le coup, mais plutôt le résultat d'un processus d'examen à plusieurs niveaux avant l'étape de la présentation par un avocat du ministère public ayant une certaine compétence en la matière. Voilà pourquoi les décisions du tribunal sur, par exemple, la nature des motifs raisonnables ou l'absence d'autres moyens d'enquête, peuvent avoir un effet sur les demandes subséquentes et empêcher la répétition de demandes inadéquates. De même, les juges qui entendent les demandes seraient amenés à prendre connaissance de cette jurisprudence.

De plus, nul ne peut douter de la réalité d'une règle d'exclusion. Contrairement aux sanctions pénales ou civiles, les juges procèdent à l'exclusion de la preuve et la police modifie ses procédures en conséquence[252].

Par ailleurs, l'exclusion de la preuve à la suite d'une audition judiciaire contribue à l'élaboration de lignes directrices, à l'intention du juge appelé à donner une autorisation, sur le respect des conditions de la demande, comme la cause raisonnable, l'absence d'autres moyens d'enquête, etc., de façon à prévenir la répétition des infractions[253].

Les partisans de l'exception fondée sur la bonne foi à la règle d'exclusion font valoir que la plupart de ces buts sont atteints par une règle qui permet la recevabilité de la preuve lorsque les autorités n'ont pas agi de façon intentionnelle ou insouciante pour éviter les contraintes de la loi, sans imposer le coût élevé qui découle d'une règle d'exclusion absolue. En fait, il s'agit d'appliquer un certain critère d'équilibre. Cet argument semble particulièrement valable lorsque la police a agi de bonne foi en se fondant sur un mandat (ou une autorisation, dans le cadre de la surveillance électronique). Schroeder affirme ce qui suit :

---

247. Mertens et Wasserstrom, *loc. cit. supra*, note 240, p. 445-446.

248. Voir Schroeder, *loc. cit. supra*, note 240, p. 1384.

249. Voir, par exemple, *R.* v. *Collins*, (1985) 5 C.C.C. (3d) 141 (C.A. C.-B.).

250. Voir Dallin H. Oaks, «Studying the Exclusionary Rule in Search and Seizure», (1970) 37 *U. Chi. L. Rev.* 665; Schroeder, *loc. cit. supra*, note 240, p. 1378-1382; Davies, *loc. cit. supra*, note 245, spécialement aux pages 627-629.

251. Voir Schroeder, *loc. cit. supra*, note 240, p. 1384.

252. Voir Mertens et Wasserstrom, *loc. cit. supra*, note 240, p. 400-401.

253. Les partisans de la règle d'exclusion du quatrième amendement jugent qu'il s'agit là d'une fin importante de la règle; voir Mertens et Wasserstrom, *loc. cit. supra*, note 240, p. 401-406; Wayne R. LaFave, *Search and Seizure*, St. Paul, Minn., West Publishing, 1978, vol. 1, 1984 Pocket Part, p. 13-18; Stewart, *loc. cit. supra*, note 232, p. 1400-1401.

[TRADUCTION]
Des problèmes particuliers en matière d'utilisation d'un critère fondé sur la bonne foi surgissent lorsqu'un agent demande et obtient un mandat de perquisition. Un mandat de perquisition exécuté *en conformité avec les conditions du mandat* suppose nécessairement de la bonne foi, à moins que la police ne présente au magistrat une version déformée des faits afin d'obtenir le mandat. Il arrive souvent, toutefois, que l'avocat qui prépare l'affidavit et qui présente la demande de mandat, ou que le magistrat qui délivre le mandat, fassent des erreurs susceptibles d'entraîner l'invalidité de toute la perquisition. Lorsque la police a présenté à un juge ou à un magistrat une demande de mandat en bonne et due forme, puis exécuté ce mandat dans le respect strict des conditions énoncées, l'exclusion de la preuve ainsi obtenue ne peut avoir aucun effet de dissuasion à l'égard de la conduite future de la police. Bien sûr, l'exclusion de la preuve pourrait améliorer les décisions des juges qui lancent des mandats pour la forme ou qui n'ont pas les qualités nécessaires pour évaluer de façon intelligente la preuve produite. Cependant, même les magistrats consciencieux et au fait du droit peuvent parfois faire des erreurs; en pareil cas, l'exclusion n'a absolument aucune valeur de dissuasion. Il convient donc de retenir la règle de l'exclusion de la preuve seulement dans le cas des perquisitions faites sans mandat et des perquisitions effectuées en vertu de mandats fondés sur de faux témoignages ou des éléments de preuve si insuffisants qu'aucun magistrat raisonnable n'aurait pu y croire. Cela devrait encourager une utilisation de bonne foi des mandats tout en protégeant les personnes contre l'abus des procédures de mandat[254]. [C'est nous qui soulignons]

Le débat ne comporte cependant pas uniquement des arguments favorables à l'exception de la bonne foi, car on a présenté des arguments en faveur d'une règle d'exclusion plus large[255].

L'un des problèmes soulevés est celui de la recherche du juge le plus favorable, qui pourrait constituer une faiblesse grave d'une règle fondée sur la bonne foi comme celle énoncée dans notre formule «B». La légitimité de cette solution dépend de la neutralité du juge appelé à donner une autorisation; il doit être en mesure de rejeter les demandes inadéquates. La recherche du juge le plus favorable suppose qu'un procureur peut choisir le juge qui déterminera la validité de la demande d'autorisation, et cela parce que le juge est partial, «qu'il penche en faveur de la Couronne ou de la police» ou tout simplement qu'il manque d'expérience et qu'il est par conséquent susceptible d'être impressionné par la teneur de la demande et la compétence de la police et de l'agent désigné. Dans le cas d'une demande de qualité douteuse ou de très grande importance, on se trouve ainsi à réduire le risque d'un refus. D'un point de vue plus positif, on peut choisir un juge en raison de sa compétence, afin de s'assurer que tout est en ordre et qu'il n'y aura pas de difficultés par la suite. Cela est important lorsque l'on prévoit que les poursuites découlant de l'autorisation feront l'objet d'une lutte juridique très serrée et que les documents seront scrutés de très près.

Les dispositions sur le secret entraînent notamment l'inconvénient suivant : d'une part, il est impossible de déterminer la fréquence de la recherche du juge le plus favorable, tandis que, d'autre part, ce même secret encourage la perception selon laquelle

254. Schroeder, *loc. cit. supra*, note 240, p. 1418-1419.

255. Voir, à titre indicatif, l'opinion dissidente dans *United States* v. *Leon*, *supra*, note 211; Stewart, *loc. cit. supra*, note 232, p. 1403; Mertens et Wasserstrom, *loc. cit. supra*, note 240; LaFave, *op. cit. supra*, note 253, p. 11-15.

cette pratique est courante. Au fond, cependant, et malgré les prétentions contraires, nous croyons que la recherche du juge le plus favorable repose sur la seule spéculation[256]. Dans son acception la plus négative, elle suppose la mauvaise foi de la part de l'agent et du juge, et nous éprouvons de la réticence à rejeter, sur la seule foi d'une telle spéculation, une règle qui comporte beaucoup de mérites.

Cette prise de position ne minimise cependant en rien l'importance de la perception selon laquelle cette pratique existe. Comme nous l'avons déjà souligné plus haut, cette perception, qui est toujours présente à l'égard des procédures *ex parte*, est renforcée lorsque les procédures sont secrètes à jamais et qu'il n'y a aucune consignation de leur déroulement. Nous ne voudrions pas que le régime que nous proposons soit menacé par la *perception* voulant que les garanties qu'il contient seront minées par la recherche du juge le plus favorable. Puisque nous recommandons que les documents présentés lors de la demande soient éventuellement communiqués au défendeur, cela devrait résoudre en partie le problème. Comme moyen d'éliminer cette perception, on a suggéré de suivre l'exemple donné par l'*Administrative Office* des tribunaux des États-Unis dans le rapport sur les tables d'écoute[257], et de publier le nom des juges ainsi que le nombre d'autorisations qu'ils accordent. La Commission a soumis cette suggestion aux personnes qu'elle consulte, et leur réponse n'a pas été très enthousiaste. De plus, il n'est pas sûr que cette façon de procéder contribue à l'élimination de la recherche du juge le plus favorable.

Nous préférons que le problème soit traité directement, et nous espérons voir la mise en place de règles administratives qui établissent un système de rotation. Dans un tel système, le procureur du ministère public doit tout simplement accepter le juge nommé pour entendre les demandes d'autorisation. Il est évident que ce système ne peut fonctionner de façon efficace dans une circonscription de petite taille, mais en pareil cas, les possibilités de recherche du juge le plus favorable sont très réduites. Nous connaissons aussi l'existence, dans quelques grandes circonscriptions, de systèmes où un groupe de juges sont désignés. Pourvu que les juges ne se sentent pas partie avec le ministère public en raison de la fréquence avec laquelle ils entendent de telles demandes, nous jugeons qu'un tel système, destiné à encourager l'acquisition de compétence par les juges appelés à donner une autorisation, ne va pas à l'encontre de notre recommandation. Nous ne jugeons cependant pas opportun d'en faire une recommandation formelle.

En acceptant la critique émise par le juge Stewart et d'autres personnes, et en tenant compte des niveaux d'autorité qui entrent en jeu dans une demande d'écoute électronique, ne pourrait-on pas déduire que la version limitée de l'exception fondée sur la bonne foi qui est énoncée dans la formule «B» est un compromis satisfaisant?

---

256. Par contre, voir Cohen, *op. cit. supra*, note 97, p. 140-143, et les références qui s'y trouvent, notamment le *U.S. Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance* (1976), p. 73-74.

257. *Supra*, note 150.

Un tel critère éliminerait les pires abus, et la possibilité d'une enquête judiciaire écarterait certaines demandes irrégulières. Il se développerait une jurisprudence pour guider les juges appelés à donner une autorisation, puisqu'une décision sur la bonne foi exige une analyse des critères appropriés. On pourrait écarter le danger que l'exception de la bonne foi devienne un encouragement à l'ignorance, en excluant de la définition de la bonne foi le défaut, par insouciance, de respecter les conditions prévues par la loi. Somme toute, *dans le domaine de la révision de l'autorisation en raison de vices de fond dans la demande*, nous préférons l'exception fondée sur la bonne foi à l'exclusion de la preuve comme mécanisme primaire d'application de la loi.

E. La preuve dérivée

La preuve dérivée est l'élément de preuve, autre que la communication privée elle-même, qui est obtenu par suite de l'acquisition de la communication privée. À l'heure actuelle, l'article 178.16 contient la règle d'exclusion limitée suivante :

> (1) Une communication privée qui a été interceptée est inadmissible en preuve contre son auteur ou la personne à laquelle son auteur la destinait à moins
>
> *a*) que l'interception n'ait été faite légalement, ou
>
> *b*) que l'auteur de la communication privée ou la personne à laquelle son auteur la destinait n'ait expressément consenti à ce qu'elle soit admise en preuve,
>
> toutefois les preuves découlant directement ou indirectement de l'interception d'une communication privée ne sont pas inadmissibles du seul fait que celle-ci l'est.
>
> (2) Par dérogation au paragraphe (1), le juge ou le magistrat qui préside à une instance quelconque peut refuser d'admettre en preuve des preuves découlant directement ou indirectement de l'interception d'une communication privée qui est elle-même inadmissible s'il est d'avis que leur admission en preuve ternirait l'image de la justice.

Dans l'article 178.16, la règle est exprimée en termes larges puisqu'elle s'applique à des preuves découlant directement ou indirectement de l'interception. Toute règle sur la preuve dérivée peut entraîner des problèmes complexes, notamment ceux qui suivent :

a) Si la preuve dérivée a été obtenue de deux sources, dont une seule est entachée d'un défaut, est-il possible d'en demander l'exclusion?

b) À qui incombe le fardeau de démontrer qu'il s'agit d'une preuve dérivée?

c) La preuve dérivée devrait-elle faire l'objet d'une exclusion automatique?

d) La délivrance d'un renouvellement ou d'une nouvelle autorisation suffit-elle à éliminer le défaut, de la suite des procédures?

Quelques-unes de ces questions ont été étudiées par le juge Borins, de la Cour de comté, dans l'affaire *R.* v. *Samson (No. 6)*[258]. Dans cette affaire, le juge a déterminé qu'une grande partie de la preuve présentée par le ministère public découlait directement ou indirectement d'une preuve primaire irrecevable. Il était d'avis qu'il incombait au ministère public de démontrer que sa preuve n'était pas dérivée. De plus, il n'importait aucunement que la preuve ait pu être obtenue d'autres sources. La question posée est la suivante : comment, dans les faits, a-t-elle été obtenue? La preuve obtenue de plusieurs sources (certaines entachées d'illégalité, d'autres légales) était également une preuve dérivée. Il a de plus conclu que la preuve obtenue en vertu d'une autorisation subséquente était également dérivée si la demande d'une autorisation subséquente était fondée sur des interceptions illégales. Dans l'appel interjeté par le ministère public[259], ces questions n'ont pas été étudiées parce que le tribunal a déterminé que la preuve primaire était recevable.

Dans l'étude de ces questions, nous pouvons nous inspirer de deux tendances de l'expérience américaine. Il y a tout d'abord l'expérience relative aux dispositions du Title III, en particulier de l'article 2515 qui stipule ce qui suit : [TRADUCTION] «Lorsqu'une communication téléphonique ou orale a été interceptée, aucune partie de son contenu ni aucune preuve dérivée de celle-ci ne peut être reçue en preuve dans un procès ... si la divulgation de cette information est susceptible de déroger au présent chapitre». Vient ensuite la doctrine appelée [TRADUCTION] «le fruit de l'arbre empoisonné» que l'on trouve dans la jurisprudence relative au quatrième amendement. En fait, le Congrès a manifesté sa volonté d'appliquer les principes du fruit de l'arbre empoisonné aux questions de la preuve dérivée en vertu de l'article 2515[260]. En général, il incombe à l'accusé de démontrer, par une prépondérance de la preuve, que la preuve du ministère public est entachée en raison d'une interception illégale. Cependant, la preuve entachée d'un défaut peut inclure des interceptions effectuées en vertu d'une ordonnance, qui avait elle-même été obtenue grâce à l'utilisation de preuves entachées, et si l'ordonnance initiale était viciée, tout renouvellement est automatiquement vicié[261].

Des questions délicates peuvent se poser lorsqu'il s'agit d'appliquer les règles dites d'atténuation élaborées en vertu du quatrième amendement. Ainsi, lorsque l'existence d'un témoin est mise à jour grâce à une interception illégale, quand peut-on dire que les déclarations de ce témoin sont entachées d'un vice et par conséquent irrecevables[262], et quels documents l'accusé a-t-il le droit de consulter afin d'être en mesure de se décharger du fardeau d'établir la preuve du défaut[263]?

---

258. *Supra*, note 102.

259. *R.* v. *Samson*, *supra*, note 58.

260 Voir «The Legislative History of Title III, Senate Report No. 1097», figurant à l'annexe B de l'ouvrage de David Watt, *Law of Electronic Surveillance in Canada*, Toronto, Carswell, 1979, p. 378-379.

261. Voir *United States* v. *Giordano*, *supra*, note 171.

262. Voir *United States* v. *Ceccolini*, 435 U.S. 268 (1978).

263. Voir *Alderman* v. *United States*, 394 U.S. 165 (1969). Pour une étude en détail de toutes ces questions dans le cadre de la surveillance électronique, voir J.G. Carr, *op. cit. supra*, note 67, chapitre 6.04.

La tendance récente de la Cour suprême des États-Unis est de réduire la portée de la doctrine du «fruit de l'arbre empoisonné» dans la législation relative au quatrième amendement. Cette attitude entraîne un effet direct sur les litiges pour vice de procédure en vertu du Title III. La Cour a atteint ce résultat en donnant une étendue plus grande aux règles d'atténuation. D'après une formulation récente de cette règle que l'on trouve dans l'affaire *Segura* v. *United States*[264], il n'y a pas lieu d'exclure la preuve si elle est [TRADUCTION] «atténuée au point de dissiper le défaut».

Au Canada, il existe deux variantes approximatives de la doctrine de l'arbre empoisonné. D'une part, la preuve matérielle obtenue à la suite d'un aveu illégal est admissible — c'est la règle établie dans l'affaire *St. Lawrence*[265]. De même, la disposition prévoyant «qu'aucun tort important ... ne s'est produit», énoncée au sous-alinéa 613(1)*b*)(iii) du *Code criminel*, qui permet le rejet d'un appel nonobstant la présence d'erreurs de droit au procès, est une sorte de règle d'atténuation. Par conséquent, l'expérience canadienne ne nous permet pas vraiment de tirer des conclusions. À notre avis, la fin première de la règle de la preuve dérivée dans le régime de la surveillance électronique est de décourager la dérogation volontaire aux procédures et aux garanties prévues par la loi. Lorsque le projet de loi sur l'écoute électronique a été présenté pour la première fois, la police a fait valoir que la fin première des tables d'écoute était d'obtenir des renseignements, c'est-à-dire d'obtenir d'autres preuves d'activités criminelles, et non pas nécessairement d'utiliser les communications privées interceptées elles-mêmes. Nous ne voudrions pas promouvoir un système en vertu duquel la police effectuerait des interceptions illégales à des fins d'obtention de renseignements sans craindre que la preuve qui en découle soit irrecevable. Cela minerait toutes les garanties intégrées au mécanisme prévu par la loi, et serait susceptible de déconsidérer l'administration de la justice.

D'autre part, nous cherchons ardemment à éviter la complexité qui semble inévitablement découler de toute règle de la preuve dérivée. À notre avis, une bonne partie de la complexité du mécanisme en vigueur aux États-Unis découle de la règle de l'exclusion automatique de la preuve dès qu'il est établi que celle-ci est entachée d'un vice. C'est pour cette raison que les tribunaux s'efforcent de sortir la preuve du cadre de la règle d'exclusion en cas de vice. Par conséquent, si nous pouvions donner aux tribunaux le pouvoir discrétionnaire d'exclure la preuve tout en leur offrant quelques règles simples sur la nature de la preuve dérivée, il y aurait peut-être moyen, du moins le souhaitons-nous, d'éviter certains de ces problèmes.

F. La longueur des procédures

Depuis l'adoption de la Partie IV.1, on a exprimé des réserves sur la longueur des procédures de voir-dire. La surveillance électronique est un mécanisme d'investigation très attentatoire auquel il a fallu adjoindre des contrôles stricts. Par conséquent,

264. *Segura* v. *United States*, 104 S.Ct. 3380 (1984); voir l'opinion du juge Burger, p. 3386.

265. *Supra*, note 79 et *R.* c. *Wray*, *supra*, note 8.

la preuve du respect de ces contrôles consomme du temps. De même, les preuves sont parfois très techniques, et les arguments légaux très complexes. Même si nous devons nous préoccuper de l'efficacité des procédures judiciaires, il importe que celle-ci ne nuise pas au droit de tout citoyen à un procès équitable. Nous pensons avoir rationalisé le processus de révision sans pour autant avoir empiété sur les principes fondamentaux du droit à un procès équitable et du respect de la vie privée. Nous avons tenté de limiter les questions de recevabilité aux questions de fond qui ressortissent à la raison d'être des mesures de contrôle.

Lorsque la défense désire remettre en cause tous les points en litige dans une affaire d'écoute électronique, la preuve peut comprendre le témoignage relatif à l'installation du dispositif, à la surveillance de ce dispositif, à la préparation des bandes et des transcriptions, à la continuité, à l'identification de la voix, à la preuve de la désignation des agents, et ainsi de suite. L'expérience démontre que l'avocat de la défense renonce souvent à la preuve de bon nombre de ces points lorsque ceux-ci ne sont d'aucune utilité pour la défense de son client. Nous avons inclus certaines recommandations visant à rationaliser des aspects de l'enquête et de la preuve qui ne font habituellement pas l'objet de contestation.

RECOMMANDATIONS

57. Le préavis raisonnable prévu au paragraphe 178.16(4) devrait être exigé dans tous les cas où le ministère public entend présenter une communication privée interceptée.

58. Lorsque le ministère public a omis de donner un préavis raisonnable, le juge présidant l'enquête préliminaire ou le juge du procès devrait pouvoir ajourner l'instance afin d'obliger le ministère public à donner un tel préavis, et prendre toute autre mesure nécessaire pour s'assurer que le préavis raisonnable est donné avant le début des procédures, compte tenu du droit de l'accusé de subir son procès dans un délai raisonnable.

59. L'article 457.3 devrait être modifié par l'adjonction de la disposition suivante à l'alinéa *d*.1) :

> **le juge de paix peut admettre en preuve par écrit, de vive voix, ou sous forme d'enregistrement, une communication privée qui a été apparemment interceptée au sens de la Partie IV.1 ou tout élément de preuve obtenu par suite d'une telle interception; l'article 178.16 ne s'applique pas au présent article.**

60. Les preuves primaires obtenues grâce à la surveillance électronique devraient être irrecevables sauf si :

a) l'interception a été légalement effectuée

(i) avec le consentement d'une personne qui a participé à la communication,

(ii) en conformité avec les conditions d'une autorisation;

b) une personne qui a participé à la communication consent à leur réception en preuve.

61. Le juge du procès devrait être tenu de recevoir les preuves primaires obtenues en conformité apparente avec une autorisation ou un renouvellement entachés d'un vice manifeste, sauf si les agents ne pouvaient raisonnablement croire en la validité de l'autorisation ou du renouvellement.

62. Pour l'application de la recommandation 51, la demande devrait être considérée comme entachée d'un vice de fond si, en raison d'énoncés dans la demande ou l'affidavit qui, à la connaissance des enquêteurs, étaient faux, d'énoncés qui ont été faits sans que l'on se soucie de leur véracité ou de leur fausseté, ou d'omissions délibérées ou faites par insouciance, il est établi

a) qu'aucune des conditions préalables énoncées à l'alinéa 178.13(1)*b*) n'existait;

b) que l'on n'avait aucun motif raisonnable et probable de croire qu'une personne désignée dans l'autorisation était en train de commettre l'infraction visée;

c) qu'il existe d'autres raisons permettant raisonnablement de conclure que si la véritable situation avait été connue, l'autorisation n'aurait pas été accordée, ou qu'elle l'aurait été sous une forme substantiellement différente.

63. Les preuves qui sont dérivées de preuves primaires irrecevables devraient être elles-mêmes irrecevables si, de l'avis du tribunal et eu égard à toutes les circonstances, le fait de les recevoir en preuve serait susceptible de déconsidérer l'administration de la justice.

64. Toute preuve devrait être tenue pour dérivée d'une preuve primaire dans le cas où elle n'aurait pu être obtenue sans l'acquisition de cette dernière. Ne constitue pas, toutefois, une preuve dérivée

a) celle qui est obtenue en vertu d'une autorisation valide par ailleurs, même si celle-ci est fondée sur les éléments de preuve obtenus grâce à une autorisation invalide;

b) celle qui consiste dans la déposition d'une personne qui a assisté à la perpétration d'une infraction, même si l'identité du témoin a été découverte par le moyen d'une preuve primaire inadmissible.

65. Lorsqu'une preuve primaire est déclarée irrecevable, le ministère public devrait être tenu de préciser, le cas échéant, quels éléments de preuve en sont dérivés et les raisons pour lesquelles tout autre élément de preuve n'en est pas dérivé. Pour déterminer le bien-fondé de ces raisons, le ministère public ou le prévenu devrait pouvoir, avec l'autorisation du tribunal, citer tout témoin pour

le contre-interroger, et le prévenu, avec l'autorisation du tribunal, devrait pouvoir examiner toute bande ou transcription relative à l'enquête, qu'il ait ou non participé à la communication interceptée.

66. Les preuves par affidavit devraient être recevables et, sauf preuve contraire, devraient permettre d'établir les faits suivants :

a) les lieux et les moments de l'interception;

b) la garde et la continuité des enregistrements;

c) le mode d'interception;

d) la signification du préavis.

67. Toute copie de l'autorisation signée par un juge devrait être recevable sans qu'il soit nécessaire d'établir l'authenticité de la signature.

68. La description, dans une autorisation, du statut de l'agent désigné devrait constituer la preuve de sa désignation.

VI. Recommandations diverses

A. Les rapports annuels : l'article 178.22

En vertu de l'article 178.22 du *Code criminel*, le solliciteur général ou le procureur général de la province est tenu de préparer un rapport de nature statistique. La Commission a déjà relevé les lacunes relatives au rapport prévu à l'article 178.22[266], et étudié diverses recommandations visant à augmenter la responsabilité dans ce domaine. On nous a également déclaré que le ministère de la Justice entend soumettre certaines recommandations en la matière. Malheureusement, ces recommandations ne sont pas encore prêtes, et il nous est difficile d'évaluer l'impact de nos autres recommandations destinées à accroître la responsabilité.

Malgré le fait que l'on peut obtenir des renseignements utiles en analysant des données statistiques, nous espérons que certaines de nos recommandations visant la divulgation des documents et la signification du préavis contribueront à accroître dans l'ensemble du processus le degré de transparence et de responsabilité, et à réduire en conséquence la nécessité de recourir à des statistiques. Nous n'avons donc pas jugé bon, pour le moment, de faire des recommandations pour la modification de l'article 178.22.

266. Savage, *op. cit. supra*, note 44.

B. L'avis en vertu de l'article 178.23

En vertu de l'article 178.23 du *Code criminel*, le ministre au nom duquel la demande d'autorisation a été présentée est tenu de donner, dans un délai précis, un avis par écrit, à la personne qui a fait l'objet de l'interception. Il n'existe par conséquent aucune obligation d'aviser la personne qui a fait l'objet d'une interception avec consentement, c'est-à-dire dans le cas d'une interception exécutée sans autorisation judiciaire. De par sa nature même, une interception exécutée adéquatement suppose que les personnes visées ne sont en aucun temps conscientes de l'opération, surtout s'il n'y a jamais d'accusation. Cet exemple illustre le besoin d'une forme quelconque d'avis postérieur à l'interception.

L'article 178.23 du *Code criminel* tel qu'il est interprété à l'heure actuelle prévoit seulement que la personne qui a fait l'objet de l'interception doit être avisée de ce fait. Comme la Cour en a décidé dans l'affaire *Re Zaduk and The Queen*[267], la personne n'a aucunement droit à un avis plus détaillé, où figurerait la mention de la date ou de la période de l'interception, ni à une copie de l'autorisation ou à l'accès aux enregistrements. La législation américaine exige un avis plus détaillé et donne aux tribunaux le pouvoir d'ordonner une divulgation plus complète :

> [TRADUCTION]
>
> Paragraphe 2518(8)
>
> *d*) Dans un délai raisonnable, ne dépassant pas quatre-vingt-dix jours après le dépôt d'une demande d'ordonnance d'approbation en vertu de l'alinéa 2518(7)*b*) qui est refusée, ou l'expiration de la période d'une ordonnance ou d'un renouvellement de celle-ci, le juge qui accorde ou qui refuse la demande doit faire signifier aux personnes nommées dans l'ordonnance ou la demande, et à toutes les autres personnes qui ont participé aux communications interceptées selon qu'il l'estime utile dans l'intérêt de la justice, un état où figurent les renseignements suivants :
>
> (i) le fait de la présentation de l'ordonnance ou de la demande;
>
> (ii) la date de la présentation et la période de l'interception autorisée, approuvée ou désapprouvée, ou le rejet de la demande; et
>
> (iii) le fait qu'au cours de la période visée, des communications téléphoniques ou orales ont été ou non interceptées.
>
> Sur présentation d'une requête, le juge peut, s'il l'estime approprié dans l'intérêt de la justice, communiquer à ces personnes ou à leurs conseillers juridiques, à des fins d'examen, des parties des communications interceptées, des demandes et des ordonnances. Sur présentation *ex parte* devant un juge compétent d'un motif suffisant de surseoir à la procédure, la signification de l'état prévu par le présent paragraphe peut être remise à plus tard[268].

Depuis l'adoption de cette disposition, presque toutes les personnes qui ont étudié la question ont exprimé des réserves à l'égard de la procédure d'avis actuellement en

267. *Supra*, note 189.

268. Title III, *supra*, note 67, par. 2518(8).

vigueur. On a fait valoir qu'en un sens, les personnes visées par l'interception seraient bien mieux de ne recevoir aucun avis, puisque l'avis prévu est tellement inadéquat qu'il est complètement inutile, et qu'il ne fait qu'engendrer de l'anxiété et de la frustration. Selon nous, il importe que l'avis prévu à l'article 178.23 corresponde aux fins qu'il vise. Il faut par conséquent identifier ces fins.

La jurisprudence a déterminé deux fins. Dans les affaires *R.* v. ***Welsh and Iannuzzi (No. 6)***[269] et ***Re Zaduk and The Queen***[270], la Cour a identifié la responsabilité politique comme une des fins. Dans l'affaire ***Zaduk***, le juge Lacourcière rattache cette responsabilité à la capacité du public [TRADUCTION] «de surveiller, de façon générale, l'application et l'effet pratique de la nouvelle législation». Il est d'avis que l'article 178.23 ne vise pas à donner un recours civil en cas d'interception illégale. Dans ses motifs, le juge souligne que la responsabilité civile découle [TRADUCTION] «d'interceptions illégales, c'est-à-dire non autorisées». Dans les motifs de sa dissidence, le juge Weatherston arrive à la conclusion contraire. Il est d'avis qu'il faut prévoir un mécanisme facilitant l'exercice des recours civils qui découleraient d'une interception illégale. Comme le juge le souligne, l'autorisation peut avoir permis certains moyens d'interception à certains endroits et non à d'autres. Si la personne ne possède pas d'autres renseignements, elle n'a aucun moyen de déterminer si les interceptions qui ont eu lieu respectaient les conditions de l'autorisation. Citons le juge Weatherston : [TRADUCTION] «Le citoyen a droit à la protection de la loi. Comment peut-il jouir de cette protection s'il ne connaît pas l'étendue de l'atteinte à ses droits?[271]»

Le problème des recours civils en cas d'interception illégale déborde le cadre du présent document. Nous n'avons donc pas étudié ce problème sous l'angle de la communication de la preuve au civil. D'autre part, nous jugeons que les principes de la révision et de la responsabilité qui ont guidé l'étude des pouvoirs de la police sont plus exigeants que les normes actuelles prévues à l'article 178.23. Prenons le cas de la police qui exécute un mandat de perquisition dans des lieux vacants. Dans le document de travail 30[272], nous recommandons qu'une copie du mandat soit apposée en un endroit adéquat du lieu inoccupé au moment de la perquisition. Un important principe de droit veut que les intrusions dans la vie privée soient justifiables et justifiés. Il faut par conséquent qu'à tout le moins, la justification apparente de l'intrusion grave par le biais de la surveillance électronique soit donnée à la personne visée. Celle-ci devrait donc avoir le droit de savoir à quel moment l'intrusion a eu lieu, et en vertu de quelle autorité. Nous sommes aussi d'avis qu'il faudrait établir un mécanisme pour assurer une communication plus complète lorsque cela est approprié. Nous jugeons que ces propositions doivent constituer un ensemble de mesures minimales dans les cas où aucune accusation n'est portée contre la personne qui a fait l'objet de l'interception, et où cette personne ne bénéficie pas de la divulgation intégrale ou de l'avis prévus à l'article 178.16.

---

269. *Supra*, note 31.

270. *Supra*, note 189, p. 332.

271. *Id.*, p. 341.

272. Document de travail sur les fouilles, les perquisitions et les saisies, *supra*, note 47, recommandation 27, p. 397.

Une décision récente du juge Steele, dans l'affaire *R.* v. *X*[273] a fait ressortir un problème dans la formulation du paragraphe 178.23(4). Cette disposition donne au juge le pouvoir de prolonger le délai pour donner l'avis jusqu'à trois ans pourvu notamment «que l'enquête au sujet de l'infraction pour laquelle l'autorisation est demandée continue». Il se peut, comme dans l'affaire *X*, que la première autorisation porte sur certaines infractions et que l'enquête soit terminée. Entre temps, l'enquête portant sur d'autres infractions pour lesquelles de nouvelles autorisations ont été obtenues peut se poursuivre. La formulation du paragraphe 178.23(4) empêcherait pourtant le juge de proroger le délai pour donner l'avis relatif à la première autorisation. À notre avis, le besoin d'une prorogation est légitime dans le dernier cas, puisque toute notification serait susceptible de nuire à l'enquête connexe qui se poursuit. Il faudrait donc modifier la loi afin d'éliminer ce problème.

Un problème supplémentaire se pose à l'égard des sanctions en cas de défaut de donner l'avis prévu à l'article 178.23. La jurisprudence considère que le défaut de donner l'avis n'a aucun effet sur la recevabilité de la preuve lorsque des accusations ont effectivement été portées à la suite de l'enquête[274].

C'est uniquement dans des circonstances exceptionnelles que l'exclusion de la preuve peut se justifier sur la base du non-respect de disposition de la loi qui ne portent pas sur la légalité de l'interception. À l'heure actuelle, le *Règlement sur la protection de la vie privée*[275] prévoit que le procureur général ou le solliciteur général doit certifier au tribunal le mode de signification de l'avis. Dans les cas où la personne n'a jamais fait l'objet d'une accusation et où, par voie de conséquence, les dispositions relatives à l'avis prévu à l'article 178.16 ne s'appliquent pas, cette exigence est suffisante, à charge d'apporter une légère modification à la formulation afin de montrer que l'exigence de certification existe non seulement «lorsqu'il a lui-même donné l'avis», mais aussi du fait que l'avis est obligatoire en vertu de l'article 178.23. Nous ne voyons aucun besoin d'une sanction particulière tant que l'on ne nous démontrera pas que le régime présent n'est pas adéquat.

Lorsque des accusations sont portées *et* qu'un avis est signifié en vertu de l'article 178.16, nous pensons que l'avis est adéquat et nous ne voyons pas la nécessité d'un avis plus détaillé en vertu de l'article 178.23, eu égard aux fins pour lesquelles cet avis est donné. Cependant, lorsque des accusations sont portées et que le ministère public n'a pas l'intention de fonder son accusation sur une preuve tirée de la surveillance électronique, il se peut que l'accusé ne reçoive jamais d'avis en vertu de l'article 178.16 et qu'il ne soit jamais au courant de l'interception, sauf en application de l'article 178.23. La connaissance de l'interception peut être un élément important de la possibilité pour l'accusé de présenter sa défense. Dans l'affaire récente *R.* v. *McLeod*[276], un

273. *R.* v. *X*, Haute cour Ont., jugement rendu par le juge Steele le 15 mai 1984 (non publié).

274. *R.* v. *Welsh and Iannuzzi (No. 6)*, *supra*, note 31; *R.* v. *Miller and Thomas (No. 4)*, (1975) 28 C.C.C. (2d) 128 (Cour de comté C.-B.).

275. *Règlement sur la protection de la vie privée*, C.R.C. 1978, vol. 5, chap. 440.

276. *R.* v. *McLeod*, C.A. Ont., le 13 avril 1982 (jugement non publié).

des suspects accusés de meurtre a invoqué le moyen de défense de l'alibi. Il faisait partie d'une bande de motards et ignorait que le repaire des motards avait fait l'objet d'une surveillance électronique. Ce n'est qu'à la suite du pourvoi en cassation de sa condamnation, et dans des circonstances fortuites, que son avocat a appris l'existence de l'enregistrement de sa conversation téléphonique la nuit du meurtre, conversation qui pouvait confirmer son alibi. La Cour d'appel a cassé sa condamnation et ordonné la tenue d'un nouveau procès fondé sur les nouveaux éléments de preuve.

De plus, tant qu'une règle d'exclusion, même limitée, est en vigueur, il est important que l'accusé soit conscient de l'existence de toute interception. Il faut établir un mécanisme comme celui qui est prévu à l'article 178.23 pour l'en aviser.

Nous avons enfin examiné la question de la nécessité de l'avis dans le cas des interceptions effectuées avec le consentement des personnes visées. Comme la signification d'un avis après l'interception est exigée en réalité parce qu'aucune des parties n'est consciente de l'interception, nous ne croyons pas que le besoin de signifier un avis dans ces cas soit aussi impérieux. Nous nous préoccupons également du danger éventuel que pourraient courir les informateurs et les autres personnes qui ont aidé la police en acceptant, peut-être à leurs risques, d'être porteurs de dispositifs électroniques. Dans ce contexte, nous ne voyons aucun besoin de signification d'un avis en dehors du cadre du procès.

Il se peut qu'après la fin de l'enquête et l'expiration du délai, la personne visée ne soit plus retrouvable. Certaines forces policières ont comme politique de signifier à personne l'avis prévu à l'article 178.23, même si la loi ne les y oblige pas, et de déposer un affidavit devant le tribunal lorsque la partie ne peut être trouvée. Nous jugeons que la procédure d'affidavit est adéquate, bien que nous soyons d'avis qu'une déclaration signée par l'agent devrait suffire.

RECOMMANDATIONS

69. Si l'avis prévu au paragraphe 178.16(4) n'a pas été donné, la loi devrait obliger la remise, à toute personne ayant été l'objet d'interceptions, d'un avis indiquant la date de celles-ci et d'une copie de l'autorisation en vertu de laquelle elles ont eu lieu.

70. Sur demande écrite du prévenu, tout juge investi du pouvoir de donner une autorisation ou le juge du procès devrait pouvoir exiger du ministère public qu'il divulgue les renseignements dont le prévenu pourrait avoir besoin pour sa défense.

71. Pour l'application de la recommandation 65, le juge devrait pouvoir obliger le ministère public à demander aux organismes chargés de l'application de la loi tous les renseignements qu'il estime opportuns.

72. La loi devrait exiger que l'avis prévu à l'article 178.23 soit donné dans les quatre-vingt-dix jours suivant l'expiration de l'autorisation ou du renouvellement, ou dans un délai plus long mais n'excédant pas trois ans si le juge est convaincu qu'en raison de la continuation de l'enquête, le fait de donner l'avis dans les quatre-vingt-dix jours ne servirait pas les intérêts de la justice.

73. Lorsqu'un avis prévu à l'article 178.23 ne peut être donné parce qu'une personne ne peut être trouvée, un agent de la paix au courant des efforts faits afin de trouver cette personne devrait produire devant le tribunal une déclaration écrite énonçant les motifs pour lesquels l'avis n'a pas été donné, de même que les efforts entrepris pour tenter de trouver la personne.

C. La divulgation des communications privées interceptées

L'article 178.2 du *Code criminel* instaure un mécanisme d'interdiction et de prévention qui régit l'utilisation et la divulgation de communications privées interceptées. En bref, l'interdiction vise l'utilisation ou la divulgation des communications privées interceptées, en tout ou en partie, ou la substance, le sens, l'objet ou l'existence, en tout ou en partie, de celles-ci, sans le consentement d'une partie à l'interception, à l'utilisation ou à la divulgation[277].

Les exceptions prévues au paragraphe 178.2(2) soustraient à l'interdiction prévue au paragraphe précédent l'utilisation ou la divulgation à des fins d'enquête ou de preuve ou dans le cadre de la fourniture de services. Nous n'avons aucune raison de nous prononcer contre le fondement de ces exceptions qui représentent à notre avis un équilibre satisfaisant entre les principes du droit à la vie privée, de l'application efficace de la loi et du droit à un procès équitable. Il existe toutefois des raisons pratiques qui, dans le prolongement des fondements susmentionnés, militent fortement en faveur d'une clarification, voire d'une expansion, des exceptions prévues au paragraphe 178.2(2).

Les enquêtes comportant de la surveillance électronique entraînent naturellement des centaines, voire des milliers d'heures d'écoute et de transcription des communications enregistrées, de même que des registres d'interception apparemment sans fin. En pareil cas, des problèmes de preuve importants surgissent couramment, et il arrive souvent que l'on doive faire appel à l'expérience des procureurs de la Couronne pour déterminer s'il est opportun d'intenter une poursuite, et le cas échéant, sous quel chef d'accusation. En fait, il est hautement souhaitable qu'un examen juridique indépendant des fruits du processus d'interception ait lieu dès les premiers stades, de façon à s'assurer que seules les affaires ayant un fondement juridique suffisant déclenchent le processus pénal. Même si elles sont suffisamment larges pour permettre la divulgation visée, les

277. *Code criminel*, par. 178.2(1).

exceptions de divulgation actuelles pour des raisons d'enquête, soit les alinéas 178.2(2)*b*) et *e*), devraient à notre avis être étendues de façon à permettre expressément cette divulgation. L'extension proposée ne compromet, à notre avis, aucun principe reconnu de droit à la vie privée, ni ne contrevient à l'esprit des recommandations que nous faisons.

Les communications privées interceptées conformément à une autorisation accordée par une autorité judiciaire canadienne compétente, peuvent à l'occasion apporter la preuve d'infractions commises entièrement au-delà de nos frontières, ou sur le point de l'être. Il existe des divergences d'opinions sur la question de savoir si les renseignements obtenus au moyen d'interceptions canadiennes autorisées judiciairement peuvent légalement être transmis à des organismes d'application de la loi étrangers. Bien qu'il semble hautement souhaitable que de tels renseignements soient communiqués aux autorités compétentes à l'étranger, ne serait-ce que pour respecter quelques-uns de nos engagements internationaux, il est tout aussi important que cette divulgation ne soit faite que pour autoriser des enquêteurs ou des agents de la paix dans certaines circonstances. En d'autres termes, une telle divulgation ne devrait être permise que lorsqu'elle est faite à des enquêteurs ou des agents de la paix dans des pays étrangers, et dans la mesure où elle fait état d'une infraction passée, actuelle ou éventuelle dans ces pays.

RECOMMANDATION

74. Le paragraphe 178.2(2) devrait être modifié de façon à créer une exemption expresse à l'interdiction prévue au paragraphe 178.2(1) dans les cas suivants :

a) lorsque la divulgation est faite à un agent de la paix, au *procureur général ou à son mandataire*, et qu'elle vise les intérêts de la justice; et

b) lorsque la divulgation est faite à un enquêteur ou à un agent de la paix dans un pays étranger et qu'elle vise à révéler une infraction passée, actuelle ou éventuelle dans ce pays.

D. L'aide dans l'exécution des ordonnances

Des problèmes difficiles surgissent dans l'exécution d'autorisations judiciaires lorsqu'il faut obtenir l'aide de responsables dans des locaux où les interceptions doivent avoir lieu, et d'entreprises de téléphonie, de télégraphie ou de télécommunications. Il arrive, par exemple, et ceci tout particulièrement dans les provinces de l'Ontario et du Québec, que les interceptions autorisées en vertu d'une ordonnance judiciaire ne puissent être exécutées parce que l'information et l'aide nécessaires n'ont pas été fournies par le service des communications en cause. Les tribunaux se sont prononcés sur la nécessité et la portée de l'intrusion dans la vie privée, mais l'absence d'aide retarde à tout le moins l'exécution de l'ordonnance, et la fait parfois échouer complètement.

Des arguments semblables ont été avancés plus tôt à l'égard de l'entrée clandestine dans des lieux. Par analogie, nous ne voyons pas comment l'on peut, d'une part, autoriser explicitement quelqu'un à entrer dans des lieux pour y installer des dispositifs d'interception afin d'exécuter une autorisation, et en même temps, retirer cette autorisation lorsqu'on a uniquement besoin d'une aide dans une activité qui ne nécessite pas vraiment une introduction dans la propriété de la personne visée. Nous aimerions faire deux autres commentaires. Si l'on inclut dans la loi une disposition créant l'obligation d'apporter son concours, comme celle qui figure au paragraphe 2518(4) du Title III, il faut aussi lui adjoindre une sanction adéquate en cas de non-respect, de même qu'une exemption de responsabilité en vertu du paragraphe 178.11(2). En second lieu, la compagnie de communication devrait être remboursée selon le tarif en vigueur pour l'aide apportée.

RECOMMANDATIONS

75. Le juge qui accorde l'autorisation devrait être habilité de façon expresse à ordonner à toute personne, y compris les entreprises de communications ou de télécommunications, de même que les propriétaires, gardiens ou responsables des lieux, de fournir toute l'aide technique ou matérielle, de même que les renseignements qui peuvent raisonnablement être nécessaires pour exécuter l'interception en conformité avec l'autorisation, et à ordonner que ces personnes reçoivent juste compensation suivant le tarif en vigueur.

76. L'inobservation de l'autorisation devrait constituer un outrage au tribunal[278].

278. Voir, à titre indicatif, le paragraphe 533(2) du *Code criminel*, qui rend coupable d'outrage au tribunal quiconque omet de se conformer aux termes d'une ordonnance de communication de toute pièce aux fins d'épreuve ou d'examen scientifique ou autre.

CHAPITRE QUATRE

Sommaire des recommandations

L'infraction

1. Les infractions pour lesquelles une autorisation d'intercepter des communications privées peut être obtenue devraient continuer de figurer sur une liste dressée à cette fin. Les infractions suivantes devraient être rayées de l'actuelle liste de l'article 178.1 : *Code criminel* — art. 58 (faux ou usage de faux, etc.), al. 159(1)*a*) (documentation pornographique), al. 195(1)*a*) (proxénétisme), art. 281.1 (encouragement au génocide), art. 314 (vol de courrier), art. 331 (menaces par lettres), art. 339 (emploi du courrier pour frauder); *Loi sur l'accise* — art. 158 et 163 (distillation ou vente illégale d'eau-de-vie).

2. Il y aurait lieu d'adjoindre à la liste les infractions prévues par le *Code criminel* qui suivent : al. 195(1)*b*), *c*), *d*), *h*) et *i*) (proxénétisme), art. 305.1 (taux d'intérêt criminel), art. 381.1 (menaces de commettre une infraction contre une personne jouissant d'une protection internationale).

3. La définition du crime organisé devrait être retirée de la liste des infractions visées, mais il devrait être possible d'obtenir une autorisation relativement aux enquêtes sur les complots, les tentatives et la complicité après le fait, en ce qui a trait à une infraction désignée, ou le fait de conseiller à une personne de commettre une telle infraction, de l'y amener ou de l'y inciter.

Les communications privées

4. L'expression «communication privée» devrait être définie de la façon suivante :

> **Toute communication orale ou télécommunication faites dans des circonstances telles que toute personne y participant peut raisonnablement s'attendre à ce qu'elles ne soient pas interceptées par le moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre.**

5. Une communication devrait être considérée comme privée même si une personne qui y participe croit qu'elle pourrait faire l'objet d'une autorisation accordée par un tribunal à un organisme chargé de l'application de la loi.

6. Le paragraphe 178.11(2) devrait être modifié par l'adjonction de l'alinéa *e*) comme suit :

> **à une personne qui surveille à des fins de sécurité des communications faites par les détenus d'une prison définie par la *Loi sur les prisons et les maisons de correction*, S.R.C. 1970, chap. P-21 et d'un pénitencier défini par la *Loi sur les pénitenciers*, S.R.C. 1970, chap. P-6, lorsque le fait qu'une telle surveillance peut être effectuée est dévoilé dans une annonce placée bien en vue à l'endroit où la communication peut être faite.**

7. La définition de l'expression «dispositif électromagnétique, acoustique, mécanique ou autre» devrait être modifiée comme suit :

> **«dispositif électromagnétique, acoustique, mécanique ou autre» désigne tout dispositif ou appareil utilisé ou pouvant être utilisé pour intercepter une communication privée, mais ne comprend pas un appareil de correction auditive utilisé pour améliorer, sans dépasser la normale, l'audition de l'utilisateur lorsqu'elle est inférieure à la normale, ni un dispositif tels l'enregistreur à plume, le décodeur d'impulsions multifréquences, le voyant à diode lumineuse ou autre dispositif similaire servant à identifier le numéro de téléphone composé ou l'interlocuteur et à obtenir l'heure et la date de l'appel téléphonique sans permettre l'interception des mots ni de tout autre renseignement.**

Les dispositifs optiques

8. Devrait constituer une infraction le fait d'entrer dans un lieu privé, sans autorisation judiciaire ni consentement du propriétaire ou de l'occupant légitime, afin d'y installer un dispositif optique.

9. L'autorisation d'installer un dispositif optique devrait pouvoir être obtenue sur demande présentée à un tribunal, mais aux mêmes conditions qu'une autorisation en vue de l'installation d'un dispositif d'écoute par une entrée clandestine.

10. L'expression «dispositif optique» devrait, pour l'instant, désigner tout dispositif ou mécanisme susceptible de permettre l'observation visuelle clandestine de personnes ou d'objets.

L'interception de communications privées à l'étranger

11. La preuve primaire et dérivée obtenue grâce à une interception faite hors du Canada, peu importe le lieu d'origine de la communication privée et que l'interception ait été effectuée légalement ou non, devrait être recevable pourvu que l'interception n'ait pas été faite dans un pays étranger en contravention des lois de celui-ci et avec la connivence des autorités canadiennes.

12. Le tribunal devant qui une communication privée interceptée à l'étranger est produite en preuve ne doit mener une enquête sur l'admissibilité de cette preuve que si la personne contre laquelle on tente de la faire admettre présente des éléments de preuve qui pourraient amener le tribunal à conclure que l'interception a été faite en contravention des lois du pays étranger avec la connivence des autorités canadiennes.

13. Les dispositions actuelles du paragraphe 178.16(4) devraient s'appliquer aux éléments de preuve obtenus grâce à des interceptions effectuées à l'étranger.

La surveillance participative : l'interception consensuelle

14. Il devrait continuer d'être prévu à l'article 178.11 qu'il n'est pas illégal d'intercepter une communication privée avec le consentement exprès ou tacite d'une personne qui y participe.

15. L'infraction prévue au paragraphe 178.18(1) ne devrait pouvoir être reprochée à une personne en possession d'un dispositif, ou d'un élément de celui-ci, qu'elle utilise ou entend utiliser en vue de procéder à une interception avec le consentement d'une des personnes qui participe à la communication privée.

16. (1) Avant de procéder à l'interception visée par le présent article, le policier devrait informer la personne dont on cherche à obtenir le consentement, de son droit de refuser son consentement et de le retirer en tout temps.

(2) Le consentement visé par le présent article peut être donné soit oralement, soit par écrit.

17. La signature d'une personne sur un document l'informant de son droit de refuser son consentement et de le retirer en tout temps ou l'enregistrement d'un tel consentement constitue une preuve *prima facie* du consentement donné par la personne à l'interception.

La demande d'autorisation

18. La demande d'autorisation ou de renouvellement devrait continuer d'être présentée par écrit et d'être accompagnée par un affidavit rédigé par un policier. L'audition devrait se dérouler *ex parte* et à huis clos. Le juge devrait être habilité à assermenter le policier pour vérifier les faits supplémentaires sur lesquels s'appuie la demande. Cependant, si le juge se fonde sur de tels faits pour décider de la demande, ces faits seront consignés et placés dans un paquet scellé.

Les motifs de l'autorisation

19. L'alinéa 178.13(1)*a*) devrait être modifié. Il devrait disposer que le juge peut accorder une autorisation lorsqu'il est convaincu que cela servirait au mieux les intérêts de l'administration de la justice et l'intérêt public, compte tenu de la gravité de l'infraction qui fait l'objet de l'enquête.

Les infractions interprovinciales

20. Le paragraphe 178.12(1) devrait être modifié afin qu'une autorisation puisse être accordée lorsque les communications de la personne visée peuvent être interceptées dans la province, même s'il est allégué que l'infraction a été commise dans une autre province.

La restriction des interceptions

21. L'autorisation ne devrait être accordée qu'à l'égard des personnes dont l'interception des communications privées fera avancer l'enquête sur l'infraction, du fait de leur participation à cette infraction.

22. L'article 178.13 devrait être modifié afin que le juge puisse insérer dans l'autorisation les modalités suivantes :

a) le dispositif devrait faire l'objet d'une surveillance humaine constante pendant toute la période où l'on se propose d'intercepter ou d'enregistrer des communications privées;

b) dans toute la mesure raisonnablement possible, seules les conversations des personnes visées devraient être interceptées et enregistrées;

c) lorsque l'on se propose d'intercepter les communications à un téléphone que le public peut utiliser, l'interception devrait faire l'objet d'une surveillance humaine et être accompagnée d'une surveillance visuelle;

d) il convient de prendre des mesures raisonnables pour éviter l'interception de communications privées entre conjoints, entre les médecins et leurs patients ou des autres communications faites sous le sceau du secret professionnel;

e) il convient de prendre des mesures raisonnables pour éviter d'intercepter les communications privées des personnes visées lorsque, d'après les communications antérieures, elles ne peuvent vraisemblablement pas faire avancer l'enquête sur l'infraction;

f) l'interception devrait cesser lorsque le but de l'enquête a été atteint;

g) l'interception d'une ligne téléphonique utilisée par plusieurs personnes ne doit être réalisée que lorsque la ligne fait l'objet d'une surveillance;

h) toute autre modalité que le juge estime opportune afin de restreindre l'interception et l'enregistrement des communications privées n'ayant aucun rapport avec l'enquête.

23. L'autorisation devrait porter, comme condition, que lorsqu'on se propose d'effectuer une interception dans un lieu mentionné au paragraphe 178.13(1.1), il convient de prendre des mesures raisonnables afin de veiller à ce que les communications entre avocats et clients, protégées par le secret professionnel, ne soient ni interceptées ni enregistrées.

24. Lorsqu'il y a lieu de croire que si l'autorisation est accordée, les communications entre la personne visée et son avocat, protégées par le secret professionnel, risquent d'être interceptées, ce fait devrait être divulgué au moment où la demande d'autorisation est présentée.

25. Dans les cas où la recommandation 21 s'applique, l'autorisation devra porter, comme condition, que dans la mesure raisonnablement possible, les communications entre la personne visée et son avocat, protégées par le secret professionnel, ne doivent être ni interceptées ni enregistrées.

Les clauses générales

26. Sous réserve des dispositions de la recommandation 27, l'autorisation devrait comporter une clause désignant, par leur nom ou autrement, les personnes à l'égard desquelles il existe des motifs raisonnables de croire que l'interception de leurs communications privées pourrait faire avancer l'enquête sur l'infraction en cause, en raison de leur participation à cette infraction.

27. L'autorisation devrait en outre pouvoir comporter une clause permettant l'interception des communications privées d'une catégorie de personnes non désignées, s'il existe des motifs raisonnables de croire que cette interception pourrait faire avancer l'enquête sur l'infraction en cause, en raison de leur participation à cette infraction.

28. Sous réserve des dispositions de la recommandation 29, l'autorisation devrait restreindre les interceptions à des lieux désignés.

29. L'autorisation devrait pouvoir comporter une clause permettant l'interception de communications privées dans des lieux non désignés, mais fréquentés par des personnes connues et identifiées dans l'autorisation. Seules devraient toutefois pouvoir être interceptées dans ces lieux les communications privées auxquelles la personne connue et identifiée participe, à moins qu'un mandataire spécialement désigné à cette fin n'ait demandé par écrit au juge qui a autorisé initialement la demande de modifier celle-ci dans les plus brefs délais. La demande de modification doit être accompagnée de l'affidavit de l'agent de police énonçant les motifs de l'interception dans ces lieux, le nom des personnes dont les communications privées

sont susceptibles d'être interceptées ainsi que les raisons pour lesquelles l'interception dans ces lieux est nécessaire. Le juge peut refuser de modifier l'ordonnance ou y apporter une modification dont l'entrée en vigueur est fixée à la date où la première interception a eu lieu à la nouvelle adresse désignée, à moins qu'il ne soit pas convaincu que la demande a été présentée dans les plus brefs délais, auquel cas la modification pourra prendre effet à la date que le juge estimera opportune.

30. La loi devrait énumérer les conditions *pouvant* figurer dans l'autorisation, par exemple :

a) l'obligation d'informer périodiquement le juge ayant autorisé l'interception, au sujet de l'identité des personnes dont les communications sont interceptées en vertu d'une autorisation générale;

b) l'obligation d'informer périodiquement le juge ayant autorisé l'interception, au sujet des lieux, non désignés précisément dans l'autorisation, où l'on se livre à des interceptions.

L'entrée clandestine

31. Le juge qui délivre l'autorisation devrait être investi du pouvoir d'autoriser l'introduction dans un lieu privé sans le consentement de l'occupant en vue de l'installation, de l'enlèvement ou de la réparation d'un dispositif électromagnétique, acoustique, mécanique ou autre.

32. Le juge qui délivre l'autorisation ne devrait pouvoir donner cette autorisation que lorsque les circonstances entourant l'infraction sont graves et que l'obtention d'éléments de preuve pertinents est très probable.

33. La demande d'autorisation qui comprend l'autorisation de faire une entrée clandestine devrait énoncer les motifs pour lesquels cette entrée est nécessaire et préciser pourquoi les autres moyens moins attentatoires à la vie privée ne seraient pas suffisants dans ce cas.

34. Devrait constituer une infraction le fait d'entrer dans des lieux privés sans le consentement de l'occupant en vue d'installer, de réparer ou d'enlever un dispositif électromagnétique, acoustique, mécanique ou autre et sans l'autorisation accordée en vertu de la Partie IV.1 du *Code criminel*. Devrait également constituer une infraction le fait de retirer des lieux quelque chose que ce soit au moment de l'entrée.

35. Le policier qui effectue l'entrée clandestine ne devrait pas être autorisé à recourir à la force contre quiconque pour entrer dans les lieux ou en sortir, sauf dans la mesure nécessaire pour assurer sa propre protection ou celle des autres.

36. Le juge qui délivre l'autorisation peut ordonner ou interdire l'utilisation de certains moyens pour l'entrée clandestine.

37. Après l'enquête, le propriétaire et l'occupant des lieux devraient être avisés de l'entrée clandestine, et copie de l'ordonnance autorisant l'entrée devrait leur être donnée.

38. Des mesures raisonnables devraient être prises en vue de la réparation de tout dommage causé aux lieux ou de l'indemnisation du propriétaire pour tout dommage important non réparé.

39. La consommation d'une faible quantité d'électricité pour assurer le fonctionnement du dispositif ne devrait pas constituer une infraction criminelle.

Les renouvellements

40. Lorsque, à la connaissance du mandataire désigné ou du souscripteur de l'affidavit présenté à l'appui de la demande d'autorisation, une autorisation a déjà été donnée au sujet de la même enquête ou d'une enquête connexe, la demande devrait comporter les renseignements mentionnés à l'alinéa 178.13(3)*b*) du *Code*.

41. Toute autorisation renouvelée devrait pouvoir comporter le nom des personnes antérieurement visées par l'autorisation mais qui n'y étaient pas nommées.

42. Toute autorisation renouvelée peut permettre l'interception, dans de nouveaux lieux, de communications auxquelles participent des personnes visées par l'autorisation initiale.

43. Des modifications mineures peuvent être apportées aux conditions de l'autorisation à l'occasion d'un renouvellement, notamment les suivantes :

a) la désignation différente ou plus précise de personnes ou de lieux;

b) la modification des moyens d'interception ou la désignation de nouveaux moyens;

c) la modification des infractions visées par l'autorisation initiale ou l'adjonction d'infractions ayant un rapport manifeste avec celles-ci et entrant dans le cadre de la même enquête.

44. Toute autorisation renouvelée devrait pouvoir comporter des conditions qui ne faisaient pas partie de l'autorisation initiale et qui sont destinées à restreindre l'interception de communications n'ayant aucun rapport avec l'infraction.

45. Aucune autorisation ne devrait pouvoir être renouvelée pour une période de plus de trente jours ou, si l'on établit l'existence de circonstances particulières, de plus de soixante jours. L'expression «circonstances particulières» désigne ici des circonstances telles que vraisemblablement l'enquête ne sera pas terminée au bout de trente jours *et* qu'il serait impossible en pratique d'obtenir un autre renouvellement dans les trente jours. Lorsqu'un juge délivre un renouvellement d'une durée supérieure à trente jours, il devrait être tenu de préciser, au recto de l'autorisation, les raisons qui motivent sa décision, ainsi que les circonstances particulières de l'enquête.

46. Dans tous les cas visés à la recommandation 45, le juge devrait être tenu de s'assurer que l'obtention d'un renouvellement de l'autorisation serait impossible dans les circonstances. Le juge ne devrait en aucun cas accorder l'autorisation s'il a des motifs de croire que l'on cherche à échapper aux exigences de la recommandation 45. Si le renouvellement ne peut être obtenu pour la seule raison que le précédent renouvellement ou l'autorisation n'est plus en vigueur, la nouvelle autorisation devrait avoir une durée de trente jours à moins que l'on démontre l'existence de circonstances particulières.

47. La loi devrait énoncer une liste des conditions susceptibles d'être incluses dans l'autorisation renouvelée, par exemple les suivantes :

a) la fin obligatoire de l'interception lorsque le but de l'autorisation initiale est atteint;

b) l'obligation de présenter toute demande ultérieure de renouvellement ou d'autorisation au juge qui a accordé l'autorisation ou le renouvellement initiaux.

La vérification de l'autorisation et le secret

48. L'article 178.14 du *Code criminel* devrait être modifié pour inclure ce qui suit :

a) en plus des exceptions prévues à l'alinéa (1)*a*), donner accès aux documents du paquet scellé afin de permettre d'examiner une demande d'autorisation relative à des enquêtes connexes;

b) permettre au mandataire spécialement désigné de conserver une copie conforme de tous les documents relatifs à la demande faite en vertu de l'article 178.12 ou du paragraphe 178.13(3).

49. Lorsqu'il donne le préavis prévu au paragraphe 178.16(4), le ministère public inclut une copie de l'autorisation et des renouvellements en vertu desquels les interceptions ont eu lieu, et sous réserve d'une ordonnance de la Cour, une copie de tous les documents relatifs à une demande d'autorisation ou de renouvellement.

50. Avant de donner le préavis prévu au paragraphe 178.16(4), le mandataire spécialement désigné peut, dans une requête *ex parte* et hors cour, demander à un juge défini à l'article 482 du *Code criminel* d'émettre une ordonnance de non-divulgation de certaines parties des documents pour le motif que leur divulgation risque d'entraîner la révélation de l'identité de l'informateur ou de celle de toute personne ayant collaboré à l'enquête; dans ce dernier cas, il faut montrer que la non-divulgation de l'identité de ces personnes ne nuit pas à l'intérêt public. La demande doit être faite par écrit et être accompagnée de l'affidavit de l'agent de la paix.

51. La personne contre qui l'on cherche à faire admettre une preuve en vertu de l'alinéa 178.16(1)*a*) du *Code criminel* à la suite d'une interception effectuée

en vertu d'une autorisation ou d'un renouvellement, peut demander lors de l'enquête préliminaire ou du procès, que la preuve ou la preuve dérivée soient exclues en raison d'un vice de fond dans la demande d'autorisation ou de renouvellement. La procédure suivante devrait s'appliquer :

a) la demande devrait être faite par écrit et être accompagnée d'un affidavit (ou d'une preuve donnée de vive voix avec la permission du juge);

b) le juge ne doit tenir une enquête sur la validité de la demande d'autorisation ou de renouvellement que si la demande et la preuve y afférente, de même que les documents divulgués en vertu de la recommandation 49, soulèvent réellement, à l'égard de la demande, la question d'un vice de fond, au sens de la recommandation 62, qui pourrait entraîner l'exclusion de la preuve;

c) lorsque le juge ordonne une enquête, il incombe au ministère public de prouver au tribunal que la demande n'est entachée d'aucun vice de fond au sens de la recommandation 62;

d) l'affidavit et le témoignage de l'accusé ne peuvent être invoqués par le ministère public à l'étape de l'enquête préliminaire ou du procès.

L'autorisation en cas d'urgence : l'article 178.15

52. L'article 178.15 devrait être modifié par l'adjonction du paragraphe (6) suivant :

La recevabilité de la preuve obtenue à la suite d'une ordonnance délivrée en vertu du présent article n'est pas entachée par le fait que le dispositif électromagnétique, acoustique, mécanique ou autre a été installé avant l'obtention de l'ordonnance, lorsque l'ordonnance rendue en vertu du présent article a été obtenue à l'égard d'une infraction visée par le paragraphe 247(1) (enlèvement) et qu'aucune communication privée n'a été obtenue au moyen de ce dispositif avant l'obtention de l'ordonnance.

53. Une demande d'autorisation en cas d'urgence en vertu de l'article 178.15 devrait obligatoirement être faite par écrit, par téléphone ou par d'autres moyens de télécommunication, et il devrait y avoir consignation des faits, notamment : une déclaration des motifs pour lesquels l'autorisation ne pouvait, avec une diligence raisonnable, être obtenue en vertu de l'article 178.13; les faits justifiant l'obtention d'une autorisation, de même que les faits particuliers de l'infraction; le nom des personnes dont on cherche à intercepter les communications privées ainsi que les lieux de l'interception.

La recevabilité de la preuve relative à d'autres infractions

54. Lorsque le ministère public entend présenter, à l'enquête préliminaire ou au procès portant sur des infractions non désignées dans une autorisation, des

preuves primaires obtenues grâce à celle-ci, le juge qui préside l'instance devrait avoir l'obligation de tenir un voir-dire afin de déterminer si l'interception des preuves touchant ces infractions a été effectuée de bonne foi.

55. Pour l'application de la recommandation 54, l'expression «bonne foi» a la signification suivante :

a) au moment de la demande d'autorisation ou de renouvellement, il était raisonnablement impossible de prévoir l'obtention de preuves relatives à des infractions non désignées dans la demande;

b) si l'on prévoyait obtenir des éléments de preuve relatifs à d'autres infractions, celles-ci n'ont pas été désignées dans la demande parce qu'il ne s'agissait pas d'infractions susceptibles de donner lieu à une autorisation *et* qu'elles ne formaient pas l'objet principal de l'enquête, mais n'étaient *qu'indirectement reliées* à l'enquête sur les infractions désignées dans l'autorisation;

c) au moment de la demande ou du renouvellement, on a déclaré au juge à quelles autorités l'on entendait remettre les renseignements obtenus grâce à l'interception;

d) lorsque les éléments de preuve concernent une infraction à l'égard de laquelle il était possible d'obtenir une autorisation, et si l'on croyait possible d'obtenir des preuves de cette infraction, cette croyance a été divulguée dans les documents présentés à l'appui de la demande *et* l'infraction n'a pas été désignée dans l'autorisation pour les seules raisons suivantes :

(i) les soupçons n'étaient pas suffisants pour satisfaire au critère prévu par la loi;

(ii) l'enquête sur l'infraction en question ne constituait pas le but principal de l'enquête, mais n'en était *qu'un but secondaire*.

56. S'il n'est pas convaincu que l'interception relative aux autres infractions a été effectuée de bonne foi, le juge devrait être tenu d'écarter les preuves primaires et être autorisé à écarter les preuves dont le caractère dérivé est démontré, dès lors qu'il est persuadé que leur réception en preuve est susceptible de déconsidérer l'administration de la justice.

Le recours en cas de dérogation au régime législatif

57. Le préavis raisonnable prévu au paragraphe 178.16(4) devrait être exigé dans tous les cas où le ministère public entend présenter une communication privée interceptée.

58. Lorsque le ministère public a omis de donner un préavis raisonnable, le juge présidant l'enquête préliminaire ou le juge du procès devrait pouvoir ajourner l'instance afin d'obliger le ministère public à donner un tel préavis, et prendre toute autre mesure nécessaire pour s'assurer que le préavis raisonnable est donné avant le début des procédures, compte tenu du droit de l'accusé de subir son procès dans un délai raisonnable.

59. L'article 457.3 devrait être modifié par l'adjonction de la disposition suivante à l'alinéa *d*.1) :

le juge de paix peut admettre en preuve par écrit, de vive voix, ou sous forme d'enregistrement, une communication privée qui a été apparemment interceptée au sens de la Partie IV.1 ou tout élément de preuve obtenu par suite d'une telle interception; l'article 178.16 ne s'applique pas au présent article.

60. Les preuves primaires obtenues grâce à la surveillance électronique devraient être irrecevables sauf si :

a) l'interception a été légalement effectuée

(i) avec le consentement d'une personne qui a participé à la communication,

(ii) en conformité avec les conditions d'une autorisation;

b) une personne qui a participé à la communication consent à leur réception en preuve.

61. Le juge du procès devrait être tenu de recevoir les preuves primaires obtenues en conformité apparente avec une autorisation ou un renouvellement entachés d'un vice manifeste, sauf si les agents ne pouvaient raisonnablement croire en la validité de l'autorisation ou du renouvellement.

62. Pour l'application de la recommandation 51, la demande devrait être considérée comme entachée d'un vice de fond si, en raison d'énoncés dans la demande ou l'affidavit qui, à la connaissance des enquêteurs, étaient faux, d'énoncés qui ont été faits sans que l'on se soucie de leur véracité ou de leur fausseté, ou d'omissions délibérées ou faites par insouciance, il est établi

a) qu'aucune des conditions préalables énoncées à l'alinéa 178.13(1)*b*) n'existait;

b) que l'on n'avait aucun motif raisonnable et probable de croire qu'une personne désignée dans l'autorisation était en train de commettre l'infraction visée;

c) qu'il existe d'autres raisons permettant raisonnablement de conclure que si la véritable situation avait été connue, l'autorisation n'aurait pas été accordée, ou qu'elle l'aurait été sous une forme substantiellement différente.

63. Les preuves qui sont dérivées de preuves primaires irrecevables devraient être elles-mêmes irrecevables si, de l'avis du tribunal et eu égard à toutes les circonstances, le fait de les recevoir en preuve serait susceptible de déconsidérer l'administration de la justice.

64. Toute preuve devrait être tenue pour dérivée d'une preuve primaire dans le cas où elle n'aurait pu être obtenue sans l'acquisition de cette dernière. Ne constitue pas, toutefois, une preuve dérivée

a) celle qui est obtenue en vertu d'une autorisation valide par ailleurs, même si celle-ci est fondée sur les éléments de preuve obtenus grâce à une autorisation invalide;

b) celle qui consiste dans la déposition d'une personne qui a assisté à la perpétration d'une infraction, même si l'identité du témoin a été découverte par le moyen d'une preuve primaire inadmissible.

65. Lorsqu'une preuve primaire est déclarée irrecevable, le ministère public devrait être tenu de préciser, le cas échéant, quels éléments de preuve en sont dérivés et les raisons pour lesquelles tout autre élément de preuve n'en est pas dérivé. Pour déterminer le bien-fondé de ces raisons, le ministère public ou le prévenu devrait pouvoir, avec l'autorisation du tribunal, citer tout témoin pour le contre-interroger, et le prévenu, avec l'autorisation du tribunal, devrait pouvoir examiner toute bande ou transcription relative à l'enquête, qu'il ait ou non participé à la communication interceptée.

66. Les preuves par affidavit devraient être recevables et, sauf preuve contraire, devraient permettre d'établir les faits suivants :

a) les lieux et les moments de l'interception;

b) la garde et la continuité des enregistrements;

c) le mode d'interception;

d) la signification du préavis.

67. Toute copie de l'autorisation signée par un juge devrait être recevable sans qu'il soit nécessaire d'établir l'authenticité de la signature.

68. La description, dans une autorisation, du statut de l'agent désigné devrait constituer la preuve de sa désignation.

L'avis en vertu de l'article 178.23

69. Si l'avis prévu au paragraphe 178.16(4) n'a pas été donné, la loi devrait obliger la remise, à toute personne ayant été l'objet d'interceptions, d'un avis indiquant la date de celles-ci et d'une copie de l'autorisation en vertu de laquelle elles ont eu lieu.

70. Sur demande écrite du prévenu, tout juge investi du pouvoir de donner une autorisation ou le juge du procès devrait pouvoir exiger du ministère public qu'il divulgue les renseignements dont le prévenu pourrait avoir besoin pour sa défense.

71. Pour l'application de la recommandation 65, le juge devrait pouvoir obliger le ministère public à demander aux organismes chargés de l'application de la loi tous les renseignements qu'il estime opportuns.

72. La loi devrait exiger que l'avis prévu à l'article 178.23 soit donné dans les quatre-vingt-dix jours suivant l'expiration de l'autorisation ou du renouvellement, ou dans un délai plus long mais n'excédant pas trois ans si le juge est convaincu qu'en raison de la continuation de l'enquête, le fait de donner l'avis dans les quatre-vingt-dix jours ne servirait pas les intérêts de la justice.

73. Lorsqu'un avis prévu à l'article 178.23 ne peut être donné parce qu'une personne ne peut être trouvée, un agent de la paix au courant des efforts faits afin de trouver cette personne devrait produire devant le tribunal une déclaration écrite énonçant les motifs pour lesquels l'avis n'a pas été donné, de même que les efforts entrepris pour tenter de trouver la personne.

La divulgation des communications privées interceptées

74. Le paragraphe 178.2(2) devrait être modifié de façon à créer une exemption expresse à l'interdiction prévue au paragraphe 178.2(1) dans les cas suivants :

a) lorsque la divulgation est faite à un agent de la paix, au *procureur général ou à son mandataire*, et qu'elle vise les intérêts de la justice; et

b) lorsque la divulgation est faite à un enquêteur ou à un agent de la paix dans un pays étranger et qu'elle vise à révéler une infraction passée, actuelle ou éventuelle dans ce pays.

L'aide dans l'exécution des ordonnances

75. Le juge qui accorde l'autorisation devrait être habilité de façon expresse à ordonner à toute personne, y compris les entreprises de communications ou de télécommunications, de même que les propriétaires, gardiens ou responsables des lieux, de fournir toute l'aide technique ou matérielle, de même que les renseignements qui peuvent raisonnablement être nécessaires pour exécuter l'interception en conformité avec l'autorisation, et à ordonner que ces personnes reçoivent juste compensation suivant le tarif en vigueur.

76. L'inobservation de l'autorisation devrait constituer un outrage au tribunal.